

# ON CLASSIFICATION OF FINITE-DIMENSIONAL SEMISIMPLE HOPF ALGEBRAS.

LEONID KROP

**ABSTRACT.** We develop a mechanism for classification of isomorphism types of non-trivial semisimple Hopf algebras whose group of grouplikes  $G(H)$  is abelian of prime index  $p$  which is the smallest prime divisor of  $|G(H)|$ . We describe structure of the second cohomology group of extensions of  $\mathbb{k}C_p$  by  $\mathbb{k}^G$  where  $C_p$  is a cyclic group of order  $p$  and  $G$  a finite abelian group. We carry out an explicit classification for Hopf algebras of this kind of dimension  $p^4$  for any odd prime  $p$ . The ground field is algebraically closed of characteristic 0.

**Keywords** Hopf algebras, Abelian extensions, Crossed products, Cohomology Groups

**Mathematics Subject Classification (2000)** 16W30 - 16G99

## 0. INTRODUCTION

We work with Hopf algebras  $H$  over an algebraically closed field  $\mathbb{k}$  of characteristic 0. We let  $G(H)$  denote the group of grouplikes of  $H$ . By the freeness theorem [26]  $\dim H = m \dim \mathbb{k}G(H)$  for an integer  $m$ . We say that a prime  $p$  is small relative to a finite group  $G$  if  $p$  is the least prime divisor of  $|G|$ . Unless stated otherwise, we assume that  $H$  is semisimple of dimension  $p|G(H)|$  for a prime number  $p$ ,  $G(H)$  is abelian and  $p$  is small relative to  $G(H)$ . For brevity, we name such Hopf algebras *almost abelian*. As usual, a finite-dimensional Hopf algebra is called *trivial* if it or its dual is a group algebra. The goal of the paper is to classify semisimple, non-trivial almost abelian Hopf algebras.

We introduce more notation. We denote by  $C_p$  a cyclic group of order  $p$  and by  $\mathbb{k}G$  and  $\mathbb{k}^G$  the group algebra of  $G$  over  $\mathbb{k}$  and its dual, respectively. We will write  $\text{Ext}(\mathbb{k}C_p, \mathbb{k}^G)$  for the set of all equivalence classes of extensions of  $\mathbb{k}C_p$  by  $\mathbb{k}^G$ .

The problem just stated reduces to that of classifying *abelian extensions* of a special kind. For by a result of [13],  $\mathbb{k}G(H)$  is a normal subHopf algebra, a fact that combined with the theorem of Kac-Zhu

[9, 31] yields that  $H$  lies in  $\text{Ext}(\mathbb{k}C_p, \mathbb{k}^{G(H)})$ . We will refer to elements of  $\text{Ext}(\mathbb{k}C_p, \mathbb{k}^{G(H)})$  as Hopf algebras and extensions interchangeably.

Our main concern becomes to understand the set of isomorphism types in  $\text{Ext}(\mathbb{k}C_p, \mathbb{k}^G)$  where  $G$  is a finite abelian group and  $p$  is small relative to  $G$ . In general, that is for arbitrary finite groups  $F, G$ , there is no systematic procedure by which isomorphism classes of Hopf algebras that are extensions of  $\mathbb{k}F$  by  $\mathbb{k}^G$  can be found. One purpose of the article is to fill this gap for the case in hand. In order to formulate the statement we will require a few more notions. We write  $A_p$  for the group  $\text{Aut}(C_p)$  of automorphisms of  $C_p$ . An action  $\triangleleft$  of  $C_p$  on  $G$  is a representation  $C_p \rightarrow \text{Aut}(G)$ . Let  $\mathcal{R} = \{\triangleleft\}$  denote the set of all representations. The group  $\text{Aut}(G)$  acts naturally on  $\mathcal{R}$  by conjugation splitting  $\mathcal{R}$  into the union of sets  $\text{eq}(\triangleleft)$  of representations equivalent to  $\triangleleft$ . In turn, the group  $A_p$  also acts on  $\mathcal{R}$  via  $\triangleleft \mapsto \triangleleft^\alpha$  where, for every  $\alpha \in A_p$ ,  $a \triangleleft^\alpha x = a \triangleleft \alpha(x)$ ,  $a \in G, x \in C_p$ . This action is passed on the sets  $\text{eq}(\triangleleft)$  via  $\text{eq}(\triangleleft)^\alpha = \text{eq}(\triangleleft^\alpha)$  giving rise to classes of representations  $[\triangleleft] = \cup_\alpha \text{eq}(\triangleleft)^\alpha$ . We denote the stabilizer of  $\text{eq}(\triangleleft)$  by  $C(\triangleleft)$ .

The splitting of  $\mathcal{R}$  into the union of  $[\triangleleft]$  induces a splitting of  $\text{Ext}(\mathbb{k}C_p, \mathbb{k}^G)$ . Namely, for every  $[\triangleleft]$  we define  $\text{Ext}_{[\triangleleft]}(\mathbb{k}C_p, \mathbb{k}^G)$  as the set of all equivalence classes of extensions whose  $C_p$ -action belongs to  $[\triangleleft]$ , and then we have  $\text{Ext}(\mathbb{k}C_p, \mathbb{k}^G) = \bigcup_{[\triangleleft]} \text{Ext}_{[\triangleleft]}(\mathbb{k}C_p, \mathbb{k}^G)$ . It suffices to classify isomorphism types in each  $\text{Ext}_{[\triangleleft]}(\mathbb{k}C_p, \mathbb{k}^G)$ .

To this end we bring in the second degree Hopf cohomology group [1, 23] denoted by  $H_c^2(\mathbb{k}C_p, \mathbb{k}^G, \triangleleft)$  after the work of M. Mastnak [16]. We aim at constructing a subgroup  $\mathcal{G}(\triangleleft)$  of  $\text{Aut}(G)$  and its action on  $H_c^2(\mathbb{k}C_p, \mathbb{k}^G, \triangleleft)$  compatible with isomorphism types of extensions in the sense that for any  $\tau, \tau' \in H_c^2(\mathbb{k}C_p, \mathbb{k}^G, \triangleleft)$   $(\tau, \triangleleft)$  and  $(\tau', \triangleleft)$  give rise to isomorphic Hopf algebras iff  $\tau$  and  $\tau'$  lie on the same orbit of  $\mathcal{G}(\triangleleft)$ .

To begin with, we introduce the group  $\mathbb{A}(\triangleleft)$  of all  $C_p$ -automorphisms of  $(G, \triangleleft)$ . For every  $\alpha \in C(\triangleleft)$  we fix a  $C_p$ -isomorphism  $\lambda_\alpha : (G, \triangleleft) \xrightarrow{\sim} (G, \triangleleft^\alpha)$ . We set  $\mathcal{G}(\triangleleft)$  to be the subgroup of  $\text{Aut}(G)$  generated by  $\mathbb{A}(\triangleleft)$  and the set  $\{\lambda_\alpha | \alpha \in C(\triangleleft)\}$  if  $\triangleleft$  is nontrivial, and  $\mathcal{G}(\triangleleft) = \text{Aut}(G) \times A_p$ , otherwise.

$H_c^2(\mathbb{k}C_p, \mathbb{k}^G, \triangleleft)$  contains a distinguished subgroup  $H_{cc}^2(\mathbb{k}C_p, \mathbb{k}^G, \triangleleft)$  of (the images of) symmetric Hopf 2-cocycles parametrizing cocommutative extensions. Let us write  $H_c^2(\mathbb{k}C_p, \mathbb{k}^G, \triangleleft)/\mathcal{G}(\triangleleft)_{nc}$  for the set of  $\mathcal{G}(\triangleleft)$ -orbits not contained in  $H_{cc}^2(\mathbb{k}C_p, \mathbb{k}^G, \triangleleft)$ . Reciprocally, we let  ${}_{nc}\text{Ext}_{[\triangleleft]}(\mathbb{k}C_p, \mathbb{k}^G)/\cong$  stand for the set of isotypes of noncocommutative extensions, and we put  $\text{cl}(H)$  for the isomorphism class of  $H$ .

The principal result of the paper states: There is a bijection

$$H_c^2(\mathbb{k}C_p, \mathbb{k}^G, \triangleleft) / \mathcal{G}(\triangleleft)_{nc} \xrightarrow{\sim} {}_{nc}\text{Ext}_{[\triangleleft]}(\mathbb{k}C_p, \mathbb{k}^G) / \cong$$

given by  $(\triangleleft, \tau)\mathcal{G} \mapsto \text{cl}(H(\triangleleft, \tau))$ .

Our next concern lies with structure of  $H_c^2(\mathbb{k}C_p, \mathbb{k}^G, \triangleleft)$ . We want to find a form of  $H_c^2(\mathbb{k}C_p, \mathbb{k}^G, \triangleleft)$  with good computational properties. We need several notions. Let  $H^2(C_p, \widehat{G}, \bullet)$  be the second degree cohomology group of extensions of  $C_p$  over  $\widehat{G}$ , where  $\widehat{G}$  is the dual group with the  $C_p$ -action  $\bullet$  dual to  $\triangleleft$ , and  $H^2(G, \mathbb{k}^\bullet)$  be the Schur multiplier of  $G$ . There is a mapping  $N$  [15] acting on a  $\mathbb{Z}C_p$ -module  $M$  by  $N(m) = \phi_p \cdot m$  where  $\phi_p$  is the  $p$ th cyclotomic polynomial. We denote the kernel of  $N$  in  $M$  by  $M_N$ . The main result in the strong form states that for any odd  $p$  there is a  $C_p$ -isomorphism

$$(0.1) \quad H_c^2(\mathbb{k}C_p, \mathbb{k}^G, \triangleleft) \simeq H^2(C_p, \widehat{G}, \bullet) \times H_N^2(G, \mathbb{k}^\bullet)$$

We remark that this isomorphism can be seen as the Hopf cohomology version of the Baer's formula for cohomology of central extensions of a group  $G$  by  $C_p$  [2, p.34]. On the other hand its main utility lies in the fact that both factors in the right-hand side of it are nicely computable in any set of generators for  $G$  thanks to the classical isomorphisms  $H^2(C_p, \widehat{G}, \bullet) \simeq \widehat{G}^{C_p} / N(\widehat{G})$  and  $H^2(G, \mathbb{k}^\bullet) \simeq \text{Alt}(G)$  [15] and [2], where  $\text{Alt}(G)$  is the group of all bilinear, alternate mapping  $G \times G \rightarrow \mathbb{k}^\bullet$ . We let  $\mathbb{X}(G, \triangleleft)$  denote the right-hand side of (0.1) and call it the *classifying group* of  $\text{Ext}_{[\triangleleft]}(\mathbb{k}C_p, \mathbb{k}^G)$ . For every odd  $p$   $\mathbb{X}(G, \triangleleft)$  acquires component-wise  $\mathcal{G}(\triangleleft)$ -module structure via transport of action along the isomorphism (0.1). The new, most useful, formulation of the main theorem asserts that there is a bijection

$$\mathbb{X}(G, \triangleleft) / \mathcal{G}(\triangleleft)_{nc} \xrightarrow{\sim} {}_{nc}\text{Ext}_{[\triangleleft]}(\mathbb{k}C_p, \mathbb{k}^G) / \cong$$

where  $\mathbb{X}(G, \triangleleft) / \mathcal{G}(\triangleleft)_{nc}$  denotes the set orbits of  $\mathcal{G}(\triangleleft)$  not contained in  $\widehat{G}^{C_p} / N(\widehat{G})$ .

For  $p = 2$  less is known. We show only that the isomorphism (0.1) holds for elementary 2-groups, though it is not, in general, an  $\mathbb{A}(\triangleleft)$ -isomorphism.<sup>1</sup>

The previous related works consist of the fundamental result of D. Stefan [29] to which this article provides concrete examples, and various classification theorems. The papers [8, 9, 31, 18, 19, 20, 21] treat a number of instances of almost abelian Hopf algebras. Namely, it is known that semisimple Hopf algebras of dimension  $p$  and  $p^2$  are trivial, nontrivial Hopf algebras of dimension  $p^3$  are almost abelian and the

<sup>1</sup>See Appendix 2

number of their isomorphism types equals  $p + 1$  for every odd  $p$ , while there is a unique 8-dimensional nontrivial Hopf algebra, and for any odd  $p$   $\text{Ext}(\mathbb{k}C_2, \mathbb{k}^{\mathbb{Z}_p \times \mathbb{Z}_p})$  contains a unique Hopf algebra up to isomorphism. Information on the  $p^4$ -dimensional semisimple Hopf algebras is limited to  $p = 2$  and consists of a complete classification of 16-dimensional semisimple Hopf algebras and almost abelian Hopf algebras  $H$  of dimension  $2^{n+1}$  with  $G(H) = \mathbb{Z}_{2^{n-1}} \times \mathbb{Z}_2$  both due to Y. Kashina [10, 11].

The paper is organized in six sections. In Section 1 we review the necessary facts of the theory of abelian extension. Sections 2 and 3 are devoted to the main results. We prove the structure theorem for the groups  $H_c^2(\mathbb{k}C_p, \mathbb{k}^G, \triangleleft)$  and the isomorphism and bijection theorems in Sections 3 and 4, respectively. Section 5 contains applications to classification of Hopf algebras of dimensions  $p^2, p^3$  and an example of a non self-dual semisimple Hopf algebra of dimension  $p^3$ . However the bulk of this Section is devoted to finding the exact number of nontrivial almost abelian Hopf algebras of dimension  $p^4$ ; we show that there are  $5p + 23$  distinct almost abelian Hopf algebras, if  $p > 3$ , and 33, otherwise. In the course of the proof we extend the contents of [11] from  $p = 2$  to an arbitrary prime. In the last section we revisit a theorem of Kac-Masuoaka on 8-dimensional Hopf algebras and give a generalization of a result of A. Masuoaka [21].

**0.1. Notation and Convention.** We adhere to the notation of [24] on Hopf algebras and to [1, 16, 23] for the theory of Hopf algebra extensions. In addition to notation in the Introduction we will use the following.

$A^\bullet$  the group of units of a commutative ring  $A$ .

$\Gamma^n$  direct product of  $n$  copies of group  $\Gamma$ .

$\text{Fun}(\Gamma, A^\bullet)$  the group of all functions from  $\Gamma$  to  $A^\bullet$  with pointwise multiplication.

$Z^2(\Gamma, A^\bullet, \bullet)$ ,  $B^2(\Gamma, A^\bullet, \bullet)$  and  $H^2(\Gamma, A^\bullet, \bullet)$  are the groups of 2-cocycles, 2-coboundaries, and the second degree cohomology group of  $\Gamma$  over  $A^\bullet$  with respect to an action  $\bullet$  of  $\Gamma$  on  $A$  by ring automorphisms.

$\delta_\Gamma$  the differential of the standard cochain complex for cohomology of the triple  $(\Gamma, A^\bullet, \bullet)$  [15, IV.5].

$\mathbb{Z}_n$  cyclic group of order  $n$  additively written.

In order to simplify notation we will often use the same symbol for an element of  $Z^2(\Gamma, A^\bullet, \triangleleft)$  and its image in  $H^2(\Gamma, A^\bullet, \triangleleft)$ . The context makes the intended meaning clear.

Throughout the paper we treat the terms  $\Gamma$ -module,  $\Gamma$ -linear, etc as synonymous to  $\mathbb{Z}\Gamma$ -module,  $\mathbb{Z}\Gamma$ -linear, etc. We use the abbreviated term isotypes for isomorphism types.

## 1. ABELIAN EXTENSIONS

In this paper we are concerned with finite-dimensional Hopf algebras over  $\mathbb{k}$ . Let  $F$  and  $G$  be finite groups. A Hopf algebra  $H$  is an extension of  $\mathbb{k}F$  by  $\mathbb{k}G$  if there is a sequence of Hopf mappings

$$(1.1) \quad \mathbb{k}G \xrightarrow{\iota} H \xrightarrow{\pi} \mathbb{k}F$$

with  $\iota$  monomorphism,  $\pi$  epimorphism,  $\iota(\mathbb{k}G)$  normal in  $H$  and  $\text{Ker}\pi = \iota(\mathbb{k}G)^+H$ . We give a synopsis of basic results on abelian extensions referring to [23] for details.

An abelian extension is characterized by a quadruple  $D = \{\sigma, \tau, \triangleleft, \triangleright\}$  called a datum for  $H$  and we write  $H = H(D)$ . This comes about from a crossed product splitting of  $H$  and  $H^*$ . For by [25], or general theorems [28, 2.4], [17, 3.5]<sup>2</sup>  $H$  is a crossed product of  $\mathbb{k}F$  over  $\mathbb{k}G$ . Since  $H^*$  is an extension of  $\mathbb{k}G$  by  $\mathbb{k}F$ , see [5, 4.1] or [1, 3.3.1],  $H^*$  is a crossed product of  $\mathbb{k}G$  over  $\mathbb{k}F$ . Thus there are two module algebra actions  $\cdot : \mathbb{k}F \otimes \mathbb{k}G \rightarrow \mathbb{k}G$  and  $\cdot : \mathbb{k}F \otimes \mathbb{k}G \rightarrow \mathbb{k}F$  and a pair of group 2-cocycles  $(\sigma, \tau) \in Z^2(F, (\mathbb{k}G)^\bullet) \times Z^2(G, (\mathbb{k}F)^\bullet)$  giving  $H$  and  $H^*$  an algebra structure with the multiplication

$$(1.2) \quad (f\bar{x})(f'\bar{y}) = f(x.f')\sigma(x, y)\bar{x}\bar{y}, \quad x, y \in F, f, f' \in \mathbb{k}G$$

$$(1.3) \quad (\bar{a}\phi)(\bar{b}\phi') = \bar{(ab)}\tau(a, b)(\phi.b)\phi', \quad a, b \in G, \phi, \phi' \in \mathbb{k}F$$

The standard identification  $\mathbb{k}G \cong (\mathbb{k}G)^*$  via  $a \mapsto \text{ev}(a) : f \mapsto f(a)$  allows us to define a right action  $\triangleleft$  of  $\mathbb{k}F$  on  $\mathbb{k}G$  by the transpose of action  $\cdot$ , viz.  $\langle a \triangleleft x, f \rangle = \langle \text{ev}(a), x.f \rangle$ . That is

$$(1.4) \quad (a \triangleleft x)(f) := f(a \triangleleft x) = (x.f)(a), \text{ for all } f \in \mathbb{k}G, a \in G, x \in F.$$

Likewise we obtain an action  $\triangleright$  of  $\mathbb{k}G$  on  $\mathbb{k}F$ . In fact both  $\triangleleft$  and  $\triangleright$  are permutation actions on  $G$  and  $F$ , respectively. In the dual bases  $\{p_a | a \in G\}$  and  $\{p_x | x \in F\}$  for  $\mathbb{k}G$  and  $\mathbb{k}F$  the two pairs of actions are related by the formulas

$$(1.5) \quad x.p_a = p_{a \triangleleft x^{-1}}$$

$$(1.6) \quad p_x.a = p_{a^{-1} \triangleright x}.$$

We fuse both actions into the definition of a product on  $F \times G$  via

$$(1.7) \quad (xa)(yb) = x(a \triangleright y)(a \triangleleft y)b$$

We use the standard notation  $F \bowtie G$  for the set  $F \times G$  endowed with multiplication (1.7).

---

<sup>2</sup>A short independent proof is given in the Appendix 1

Dualizing multiplication (1.3) endows  $H$  with a coalgebra structure  $\Delta_H, \epsilon_H$  given by [23, 4.5]

$$(1.8) \quad \begin{aligned} \Delta_H(f\bar{x}) &= \sum_{a,b \in G} \tau(x, a, b) f_1 p_a \overline{b \triangleright x} \otimes f_2 p_b \bar{x}, \\ \epsilon_H(f\bar{x}) &= f(1_G). \end{aligned}$$

We say that two structures (1.2) and (1.8) are coherent if they turn  $H$  into a bialgebra. The coherence conditions are

$$(1) \ F \bowtie G \text{ is a group and } (2) \ \delta_G \sigma^{-1} = \delta_F \tau.$$

Bialgebras so defined are always Hopf algebras, see [23, 4.7] for a formula for the antipode.

In consequence the second Hopf cohomology group of extensions (1.1) with fixed actions  $\triangleleft, \triangleright$  is defined as

$$(1.9) \quad H_{\text{Hf}}^2(\mathbb{k}F, \mathbb{k}^G, \triangleleft, \triangleright) = Z_{\text{Hf}}^2(\mathbb{k}F, \mathbb{k}^G, \triangleleft, \triangleright) / B_{\text{Hf}}^2(\mathbb{k}f, \mathbb{k}^G, \triangleleft, \triangleright)$$

where  $Z_{\text{Hf}}^2(\mathbb{k}F, \mathbb{k}^G, \triangleleft, \triangleright) = \{(\sigma, \tau) | \delta_G \sigma^{-1} = \delta_F \tau\}$  is the group of Hopf 2-cocycles and  $B_{\text{Hf}}^2(\mathbb{k}f, \mathbb{k}^G, \triangleleft, \triangleright) = \{(\delta_F \zeta^{-1}, \delta_G \zeta) | \zeta : F \times G \rightarrow \mathbb{k}^\bullet\}$  is the group of Hopf 2-coboundaries.

An extension (1.1) is called cocentral [12] if  $\mathbb{k}^F$  is a central subalgebra of  $H^*$ . Some equivalent conditions are  $\triangleright$  is trivial or  $G$  is normal in  $F \bowtie G$ . Another consequence of cocentrality is that  $F$  acts by Hopf automorphisms of  $\mathbb{k}^G$  (see e.g. [19, 11]).

Our main interest lies with cocentral extensions (1.1) satisfying the condition

$$(1.10) \quad H^2(F, (\mathbb{k}^G)^\bullet, \triangleleft) = \{1\} \text{ for every action } \triangleleft.$$

We will call them *special cocentral*. Below we will write  $H = H(\tau, \triangleleft)$  for a special cocentral extension with a datum  $\{\tau, \triangleleft\}$ .

In the case of special cocentral extensions the definition of cohomology groups (1.9) can be simplified. This has been done by M. Mastnak [16] and we adopt his formulation. First we define an action of  $F$  on  $\text{Fun}(F^n \times G^m, \mathbb{k}^\bullet)$  extending the action  $\triangleleft$  of  $F$  on  $G$  via

$$(1.11) \quad y \cdot \phi(x_1, \dots, x_n, a_1, \dots, a_m) = \phi(x_1, \dots, x_n, a_1 \triangleleft y, \dots, a_m \triangleleft y).$$

Now we let  $Z_c^2(\mathbb{k}F, \mathbb{k}^G, \triangleleft)$  and  $B_c^2(\mathbb{k}F, \mathbb{k}^G, \triangleleft)$  denote the subgroups of  $Z^2(G, (\mathbb{k}^F)^\bullet, \text{id})$  and  $B^2(G, (\mathbb{k}^F)^\bullet, \text{id})$  of 2-cocycles  $\tau$  and 2-coboundaries  $\delta_G \eta$ , respectively satisfying  $\delta_F \tau = 1 = \delta_F \eta$ . This leads us to define

$$H_c^2(\mathbb{k}F, \mathbb{k}^G, \triangleleft) = Z_c^2(\mathbb{k}F, \mathbb{k}^G, \triangleleft) / B_c^2(\mathbb{k}F, \mathbb{k}^G, \triangleleft).$$

One can see immediately that the mapping  $\tau \mapsto (1, \tau)$  carries out an isomorphism between  $H_c^2(\mathbb{k}F, \mathbb{k}^G, \triangleleft)$  and  $H_{\text{Hf}}^2(\mathbb{k}F, \mathbb{k}^G, \triangleleft, \text{id})$ . Explicitly

both conditions  $\delta_F \tau = \epsilon$  and  $\delta_F \eta = \epsilon$  are expressed by:

$$(1.12) \quad \tau(xy) = \tau(x)(x.\tau(y))$$

$$(1.13) \quad \eta(xy) = \eta(x)(x.\eta(y))$$

for all  $x, y \in F$  where  $F$  acts by (1.11). The equations say that each  $\tau$  and  $\eta$  is a crossed homomorphism  $F \rightarrow \mathbb{k}^{G \times G}$  and  $F \rightarrow \mathbb{k}^G$ , respectively.

We call elements of  $Z_c^2(\mathbb{k}F, \mathbb{k}^G, \triangleleft)$  and  $B_c^2(\mathbb{k}F, \mathbb{k}^G, \triangleleft)$  *Hopf 2-cocycles* and *2-coboundaries*, respectively. We will use abbreviated notation  $Z_c^2(\triangleleft)$ ,  $B_c^2(\triangleleft)$ , etc for  $Z_c^2(\mathbb{k}F, \mathbb{k}^G, \triangleleft)$ ,  $B_c^2(\mathbb{k}F, \mathbb{k}^G, \triangleleft)$ , etc. when the groups  $G$  and  $F$  are clear from the context. We single out a subgroup  $B_{cc}^2(\triangleleft)$  of  $Z_c^2(\triangleleft)$  by the equation  $B_{cc}^2(\triangleleft) = B^2(G, (\mathbb{k}^F)^\bullet) \cap Z_c^2(\triangleleft)$ . Clearly  $B_c^2(\triangleleft) \subset B_{cc}^2(\triangleleft)$  so we can form the subgroup  $H_{cc}^2(\triangleleft) = B_{cc}^2(\triangleleft)/B_c^2(\triangleleft)$  of  $H_c^2(\triangleleft)$ . We note in passing that elements of  $H_{cc}^2(\triangleleft)$  parametrize cocommutative extensions in  $\text{Ext}(\mathbb{k}F, \mathbb{k}^G)$ .

We add a remark on  $F$ -invariance of subgroups just defined.

**Lemma 1.1.** *If  $F$  is abelian, then subgroups  $Z_c^2(\triangleleft)$ ,  $B_{cc}^2(\triangleleft)$ , and  $B_c^2(\triangleleft)$  are  $F$ -invariant.*

PROOF: For  $Z_c^2(\triangleleft)$  one has readily by (1.11)

$$(z.\tau)(xy) = (z.\tau)(x)(zx.\tau(y)) = (z.\tau)(x)(x.((z.\tau)(y)))$$

as  $x$  commutes with  $z$ . This shows  $z.\tau \in Z_c^2(\triangleleft)$ . For the remaining two cases it suffices to note that the operator  $\delta_G$  is  $F$ -linear on account of  $G$  acting trivially on  $\mathbb{k}^F$ .  $\square$

## 2. STRUCTURE OF $H_c^2(\mathbb{k}C_p, \mathbb{k}^G, \triangleleft)$

From this point on  $H$  is an almost abelian Hopf algebra,  $G = G(H)$ ,  $F = C_p$ , and  $p$  is small relative to  $G$ . Plainly  $G$  is normal in  $C_p \rtimes G$ , hence the action  $\triangleright$  is trivial. In addition,  $H^2(C_p, (\mathbb{k}^G)^\bullet, \triangleleft)$  vanishes as  $\mathbb{k}^\bullet$  is a divisible group by e.g. [16, 4.4]. All in all we see that  $H$  is a special cocentral extension of  $C_p$  by  $\mathbb{k}^G$ . We begin with a simple fact.

**Lemma 2.1.** *Let  $\tau \in Z^2(G, (\mathbb{k}^{C_p})^\bullet)$ . Then for every  $x \in C_p$   $\tau(x)$  is a 2-cocycle for  $G$  with coefficients in  $\mathbb{k}^\bullet$  with the trivial action of  $G$  on  $\mathbb{k}^\bullet$ .*

PROOF: The 2-cocycle condition for the trivial action is

$$(2.1) \quad \tau(a, bc)\tau(b, c) = \tau(ab, c)\tau(a, b).$$

Expanding both sides of the above equality in the basis  $\{p_x\}$  and equating coefficients of  $p_x$  proves the assertion.  $\square$

Consider group  $F$  acting on an abelian group  $A$ , written multiplicatively, by group automorphisms. Let  $\mathbb{Z}F$  be the group algebra of  $F$  over  $\mathbb{Z}$ .  $\mathbb{Z}F$  acts on  $A$  via

$$(\sum c_i x_i).a = \prod x_i.(a^{c_i}), \quad c_i \in \mathbb{Z}, \quad x_i \in F.$$

For  $F = C_p$  pick a generator  $t$  of  $C_p$  and set  $\phi_i = 1 + t + \cdots + t^{i-1}$ ,  $i = 1, \dots, p$ . Choose  $\tau \in Z^2(G, (\mathbb{k}^{C_p})^\bullet)$  and expand  $\tau$  in terms of the standard basis  $p_{t^i}$  for  $\mathbb{k}^{C_p}$ ,  $\tau = \sum \tau(t^i) p_{t^i}$  with  $\tau(t^i) \in Z^2(G, \mathbb{k}^\bullet)$ . An easy induction on  $i$  shows that condition (1.12) implies

$$(2.2) \quad \tau(t^i) = \phi_i.\tau(t), \quad \text{for all } i = 1, \dots, p$$

For  $i = p$  we have

$$(2.3) \quad \phi_p.\tau(t) = 1$$

in view of  $t^p = 1$  and  $\tau(1) = 1$ .

Let  $M$  be a  $\mathbb{Z}C_p$ -module. Following [15] we define the mapping  $N : M \rightarrow M$  by  $N(m) = \phi_p(t).m$ . We denote by  $M_N$  the kernel of  $N$  in  $M$ . For  $M = Z^2(G, \mathbb{k}^\bullet)$ ,  $B^2(G, \mathbb{k}^\bullet)$  or  $H^2(G, \mathbb{k}^\bullet)$  we write  $Z_N^2(G, \mathbb{k}^\bullet)$  for  $Z^2(G, \mathbb{k}^\bullet)_N$  and similarly for the other groups. We abbreviate  $Z_N^2(G, \mathbb{k}^\bullet)$  to  $Z_N^2(\triangleleft)$  and likewise for  $B_N^2(G, \mathbb{k}^\bullet)$  and  $H_N^2(G, \mathbb{k}^\bullet)$ . Thus by definition  $Z_N^2(\triangleleft)$  is the set of all 2-cocycles satisfying

$$(2.4) \quad \phi_p.s = 1.$$

We want to compare abelian groups  $Z_c^2(\triangleleft)$  and  $Z_N^2(\triangleleft)$ . This is done via the mapping

$$\Theta : Z^2(G, (\mathbb{k}^{C_p})^\bullet) \rightarrow Z^2(G, \mathbb{k}^\bullet), \quad \Theta(\tau) = \tau(t).$$

**Lemma 2.2.** *The mapping  $\Theta$  induces a  $C_p$ -isomorphism between  $Z_c^2(\triangleleft)$  and  $Z_N^2(\triangleleft)$ .*

PROOF: We begin with an obvious equality  $x.(\tau(y)) = (x.\tau)(y)$ . Taking  $y = t$  we get  $\Theta(x.\tau) = x.\Theta(\tau)$ , that is  $C_p$ -linearity of  $\Theta$ . The relations (2.2) show that  $\Theta$  is monic. It remains to establish that  $\Theta$  is epic.

Pick  $s \in Z_N^2(\triangleleft)$ . Define  $\tau : G \times G \rightarrow (\mathbb{k}^{C_p})^\bullet$  by setting  $\tau(t^i) = \phi_i(t).s$ ,  $1 \leq i \leq p$ . The proof will be complete if we demonstrate that  $\tau$  satisfies (1.12).

For any  $i, j \leq p$  we have

$$\tau(t^i)(t^i.\tau(t^j)) = (\phi_i(t).s)(t^i\phi_j(t).s) = (\phi_i(t) + t^i\phi_j(t)).s$$

One sees easily that  $\phi_i(t) + t^i\phi_j(t) = \sum_{k=0}^{i+j-1} t^k$ . Hence if  $i+j < p$  we have  $\phi_i(t) + t^i\phi_j(t) = \phi_{i+j}(t)$  and so  $\tau(t^i)(t^i.\tau(t^j)) = \tau(t^{i+j})$ . If  $i+j = p+m$



with  $m \geq 0$ , then  $\sum_{k=0}^{p+m-1} t^k = \phi_p(t) + t^p(1 + \cdots + t^{m-1})$  which implies  
 $(\sum_{k=0}^{p+m-1} t^k).s = \phi_p(t).s \cdot t^p \phi_m(t).s = \phi_m(t).s = \tau(t^{i+j})$  by (2.4) and as  
 $t^p = 1$ .  $\square$

The next step is to describe structure of  $H_{cc}^2(\triangleleft)$ . We need some preliminaries. First, we write  $x.f$  for the left action of  $C_p$  on  $\mathbb{k}^G$  dual to  $\triangleleft$  as in (1.4). Since  $\widehat{G}$  is the group of grouplikes of  $\mathbb{k}^G$ , and  $C_p$  acts by Hopf automorphisms  $\widehat{G}$  is  $C_p$ -stable. Further, we use  $\delta$  for the differential on the group of 1-cochains of  $G$  in  $\mathbb{k}^\bullet$ . We also note  $B_N^2(\triangleleft) = B^2(G, \mathbb{k}^\bullet) \cap Z_N^2(\triangleleft)$ . By (2.4)  $\delta f \in B_N^2(\triangleleft)$  iff  $\phi_p(t).\delta f = 1$  which, in view of  $\delta$  being  $C_p$ -linear, is the same as  $\delta(\phi_p(t).f) = 1$ . Since  $(\delta f)(a, b) = f(a)f(b)f(ab)^{-1}$ ,  $\text{Ker } \delta$  consists of characters of  $G$ , whence  $\delta f \in B_N^2(\triangleleft)$  iff  $\phi_p(t).f$  is a character of  $G$ . Say  $\chi = \phi_p(t).f \in \widehat{G}$ . Then as  $t\phi_p(t) = \phi_p(t)$ ,  $\chi$  is a fixed point of the  $C_p$ -module  $\widehat{G}$ . Letting  $\widehat{G}^{C_p}$  stand for the set of fixed points in  $\widehat{G}$  we have by [15, IV.7.1] an isomorphism  $H^2(C_p, \widehat{G}, \bullet) \simeq \widehat{G}^{C_p}/N(\widehat{G})$ . We connect  $B_N^2(\triangleleft)$  to  $H^2(C_p, \widehat{G})$  via the homomorphism

$$(2.5) \quad \Phi : B_N^2(\triangleleft) \rightarrow H^2(C_p, \widehat{G}, \bullet), \delta f \mapsto (\phi_p.f)N(\widehat{G})$$

**Lemma 2.3.** *The following properties holds*

- (i)  $\Theta(B_{cc}^2(\triangleleft)) = B_N^2(\triangleleft)$ ,
- (ii)  $\Theta(B_c^2(\triangleleft)) = \ker \Phi$ ,
- (iii)  $B_N^2(\triangleleft)/\ker \Phi \simeq H^2(C_p, \widehat{G}, \bullet)$ ,
- (iv)  $H_{cc}^2(\triangleleft) \simeq H^2(C_p, \widehat{G}, \bullet)$ .

PROOF: First we show that  $\Phi$  is well-defined. For,  $\delta f = \delta g$  iff  $fg^{-1} = \chi \in \widehat{G}$ , hence

$$\begin{aligned} \Phi(\delta f) &= (\phi_p.f)N(\widehat{G}) = (\phi_p.g\chi)N(\widehat{G}) \\ &= (\phi_p.g \cdot \phi_p.\chi)N(\widehat{G}) = (\phi_p.g)N(\widehat{G}) = \Phi(\delta g) \end{aligned}$$

(i) Take some  $\delta_G \eta \in B_{cc}^2(\triangleleft)$ . Evidently for every  $x \in C_p$   
 (\*)  $(\delta_G \eta)(x) = \delta(\eta(x))$ , hence  $\Theta(\delta_G \eta) = \delta(\eta(t))$  is a coboundary, and  $\phi_p.\delta(\eta(t)) = 1$  by (2.3), whence  $\Theta(\delta_G \eta) \in B_N^2(\triangleleft)$ . Conversely, pick  $\delta f \in B_N^2(\triangleleft)$  and define  $\omega = \sum_{i=1}^p (\phi_i.\delta f)p_{t^i}$ . The argument of Lemma 2.2 shows  $\omega$  lies in  $Z_c^2(\triangleleft)$ . Set  $\eta = \sum_{i=1}^p (\phi_i.f)p_{t^i}$ . Using (\*) again we derive

$$\delta_G \eta = \sum_{i=1}^p (\phi_i.\delta f)p_{t^i} = \omega,$$

hence  $\delta_G \eta \in B_{cc}^2(\triangleleft)$ . Clearly  $\Theta(\delta_G \eta) = \delta f$ .

(ii) The argument of Lemma 2.2 is applicable to 1-cocycles satisfying (1.13). It shows that  $\eta$  satisfies (1.13) iff

$$(2.6) \quad \eta(t^i) = \phi_i \cdot \eta(t)$$

For  $i = p$  we get  $\phi_p \cdot \eta(t) = \epsilon$ , hence the calculation

$$\Phi(\Theta(\delta_G \eta)) = \Phi(\delta(\eta(t))) = (\phi_p \cdot \eta(t))N(\widehat{G}) = N(\widehat{G}).$$

gives one direction. Conversely,  $\Phi(\delta f) \in N(\widehat{G})$  means  $\phi_p \cdot f = \phi_p \cdot \chi$  which implies  $\phi_p \cdot f \chi^{-1} = \epsilon$ . Set  $g = f \chi^{-1}$  and define 1-cocycle  $\eta_g = \sum_{i=1}^p (\phi_i \cdot g) p_{ti}$ . Since  $\phi_p \cdot g = \epsilon$ ,  $\eta_g$  satisfies (1.13), whence  $\delta_G \eta_g \in B_c^2(\triangleleft)$ . As  $(\delta_G \eta_g)(t) = \delta g = \delta f$  by construction,  $\Theta(\delta_G \eta_g) = \delta f$ .

(iii) We must show that  $\Phi$  is onto. For every character  $\chi$  in  $\widehat{G}^{C_p}$  we want to construct an  $f : G \rightarrow \mathbb{k}^\bullet$  satisfying  $\phi_p \cdot f = \chi$ . To this end we consider splitting of  $G$  into the orbits under the action of  $C_p$ . Since every orbit is either regular, or a fixed point we have

$$G = \cup_{i=1}^r \{g_i, g_i \triangleleft t, \dots, g_i \triangleleft t^{p-1}\} \cup G^{C_p}$$

For every  $s \in G^{C_p}$  we pick a  $\rho_s \in \mathbb{k}$  satisfying  $\rho_s^p = \chi(s)$ . We define  $f$  by the rule

$$\begin{aligned} f(g_i) &= \chi(g_i), \quad f(g_i \triangleleft t^j) = 1 \text{ for all } j \neq 1 \text{ and all } i = 1, \dots, r, \text{ and} \\ f(s) &= \rho_s \text{ for every } s \in G^{C_p} \end{aligned}$$

By definition  $(\phi_p \cdot f)(g) = \prod_{j=0}^{p-1} f(g \triangleleft t^j)$ . Therefore  $(\phi_p \cdot f)(s) = \rho_s^p = \chi(s)$  for every  $s \in G^{C_p}$ . If  $g = g_i \triangleleft t^j$  for some  $i, j$ , then a calculation  $(\phi_p \cdot f)(g) = f(g_i) = \chi(g_i) = \chi(g_i \triangleleft t^j) = \chi(g)$ , which uses the fact that  $\chi$  is a fixed point under the action by  $C_p$ , completes the proof.

(iv) follows immediately from  $H_{cc}^2(\triangleleft) = B_{cc}^2/B_c^2(\triangleleft)$  and parts (i)-(iii).  $\square$

**Corollary 2.4.** *Isomorphism  $\Theta$  induces a  $C_p$ -isomorphism  $\Theta_* : H_c^2(\triangleleft) \simeq Z_N^2(\triangleleft)/\ker \Phi$ .*

$\square$

We proceed to the main result of the section.

**Proposition 2.5.** *Suppose  $G$  is a finite abelian group. If  $|G|$  is odd, or  $G$  is a 2-group and either  $C_2$ -action is trivial, or  $G$  is an elementary 2-group, there exists a  $C_p$ -isomorphism*

$$(2.7) \quad H_c^2(\triangleleft) \simeq H^2(C_p, \widehat{G}, \bullet) \times H_N^2(G, \mathbb{k}^\bullet).$$

PROOF: (1) First we take up the odd case. By the preceeding Corollary we need to decompose  $Z_N^2(\triangleleft)/\ker \Phi$ . We note that for any  $p$  and  $G$  there is a group splitting  $Z^2(G, \mathbb{k}^\bullet) = B^2(G, \mathbb{k}^\bullet) \times H^2(G, \mathbb{k}^\bullet)$  due to the fact that the group of 1-cocycles  $\mathbb{k}^{\bullet G}$  is injective, and hence so is  $B^2(G, \mathbb{k}^\bullet)$ . We aim at finding a  $C_p$ -invariant complement to  $B^2(G, \mathbb{k}^\bullet)$ . To this end we recall a well-known isomorphism  $\underline{a} : H^2(G, \mathbb{k}^\bullet) \xrightarrow{\sim} \text{Alt}(G)$ , see e.g. [30, §2.3]. There  $\text{Alt}(G)$  is the group of all bimultiplicative alternating functions

$$\beta : G \times G \rightarrow \mathbb{k}^\bullet, \beta(ab, c) = \beta(a, c)\beta(b, c), \text{ and } \beta(a, a) = 1 \text{ for all } a \in G.$$

For the future applications we outline the construction of  $\underline{a}$ . Namely,  $\underline{a}$  is the antisymmetrization mapping sending  $z \in Z^2(G, \mathbb{k}^\bullet)$  to  $\underline{a}(z)$  defined by  $\underline{a}(z)(a, b) = z(a, b)z^{-1}(b, a)$ . One can check that  $\underline{a}(z)$  is bimultiplicative (cf. [30, (10)]) and it is immediate that  $\underline{a}$  is  $C_p$ -linear. Another verification gives  $\text{im } \underline{a} = \text{Alt}(G)$  and, moreover,  $\ker \underline{a} = B^2(G, \mathbb{k}^\bullet)$ , see [30, Thm.2.2]. Thus we obtain a  $C_p$ -isomorphism  $H^2(G, \mathbb{k}^\bullet) \simeq \text{Alt}(G)$ .

Since elements of  $\text{Alt}(G)$  are bimultiplicative mappings  $\text{Alt}(G) \subset Z^2(G, \mathbb{k}^\bullet)$ . For every  $\beta \in \text{Alt}(G)$  a simple calculation gives  $\underline{a}(\beta) = \beta^2$ . Thus  $\underline{a}(\beta) \neq 1$  as the order of  $\beta$  divides the exponent of  $G$ . It follows  $B^2(G, \mathbb{k}^\bullet) \cap \text{Alt}(G) = \{1\}$  which gives a splitting of abelian groups

$$Z^2(G, \mathbb{k}^\bullet) = B^2(G, \mathbb{k}^\bullet) \times \text{Alt}(G)$$

But now both subgroups  $B^2(G, \mathbb{k}^\bullet)$  and  $\text{Alt}(G)$  are  $C_p$ -invariant hence there holds  $Z_N^2(G, \mathbb{k}^\bullet) = B_N^2(G, \mathbb{k}^\bullet) \times \text{Alt}_N(G)$  which, in view of  $\text{Alt}(G) = H^2(G, \mathbb{k}^\bullet)$ , is the same as

$$(2.8) \quad Z_N^2(\triangleleft) = B_N^2(\triangleleft) \times H_N^2(G, \mathbb{k}^\bullet).$$

Now part (iii) of Lemma 2.3 completes the proof of (1).

(2) Here we prove the second claim of the Proposition. We decompose  $G$  into a product of cyclic groups  $\langle x_i \rangle, 1 \leq i \leq m$ . For every  $\alpha \in \text{Alt}(G)$  we define  $s_\alpha \in Z^2(G, \mathbb{k}^\bullet)$  via

$$s_\alpha(x_i, x_j) = \begin{cases} \alpha(x_i, x_j), & \text{if } i \leq j \\ 1, & \text{else.} \end{cases}$$

Since  $s_\alpha \cdot s_\beta = s_{\alpha\beta}$  the set  $S = \{s_\alpha | \alpha \in \text{Alt}(G)\}$  is a subgroup of  $Z^2(G, \mathbb{k}^\bullet)$ . One can see easily that  $s_\alpha = s_\beta \Leftrightarrow \alpha = \beta$  and  $\underline{a}(s_\alpha) = \alpha$ , hence  $S$  is isomorphic to  $\text{Alt}(G)$  under  $\underline{a}$ . For every  $z \in Z_N^2(\text{triv})$ ,  $\underline{a}(z) \in \text{Alt}_N(G)$ , and therefore  $\underline{a}(z) = \underline{a}(s)$  for some  $s \in S_N$ . We have  $zs^{-1} \in B^2(G, \mathbb{k}^\bullet)$ , but as  $zs^{-1}$  has order 2,  $zs^{-1} \in B_N^2(\text{triv})$ . Thus  $Z_N^2(\text{triv}) = B_N^2(\text{triv}) \times S_N$  which proves (2.7).

(3) We prove the last claim of the Proposition. Below  $G$  is an elementary 2-group, and action of  $C_2$  is nontrivial. First we establish an intermediate result, namely

**Lemma 2.6.** *If action  $\triangleleft$  is nontrivial, then  $Z_N^2(\triangleleft)$  is a nonsplit extension of  $\text{Alt}_N(G)$  by  $B_N^2(\triangleleft)$ .*

PROOF: This will be carried out in steps.

(i) We aim at finding a basis for  $\text{Alt}_N(G)$ . We begin by noting that as  $\text{Alt}(G)$  has exponent 2,  $\text{Alt}_N(G)$  is the set of all fixed points in  $\text{Alt}(G)$ . Put  $R = \mathbb{Z}C_2$ . One can see easily that  $R$ -module  $G$  decomposes as

$$(2.9) \quad G = R_1 \times \cdots \times R_m \times G_0$$

where  $R_i \simeq R$  as a right  $C_2$ -module, and  $G_0 = G^{C_2}$ . Denote by  $t$  the generator of  $C_2$ . For each  $i$  let  $\{x_{2i-1}, x_{2i}\}$  be a basis of  $R_i$  such that  $x_{2i-1} \triangleleft t = x_{2i}$ . We also fix a basis  $\{x_{2m+1}, \dots, x_n\}$  of  $G_0$ .

We associate to every subset  $\{i, j\}$  the bilinear form  $\alpha_{ij}$  by setting  $\alpha_{ij}(x_i, x_j) = \alpha_{ij}(x_j, x_i) = -1$ , and  $\alpha_{ij}(x_k, x_l) = 1$  for any  $\{k, l\} \neq \{i, j\}$ .

The set  $\{\alpha_{ij}\}$  forms a basis of  $\text{Alt}(G)$ . One can check easily that  $t$  acts on basic elements as follows

$$(2.10) \quad t.\alpha_{ij} = \alpha_{kl} \text{ if and only if } \{x_i, x_j\} \triangleleft t := \{x_i \triangleleft t, x_j \triangleleft t\} = \{x_k, x_l\}.$$

Recall the element  $\phi_2 = 1 + t \in \mathbb{Z}C_2$ . We define forms  $\beta_{ij}$  via

$$(2.11) \quad \beta_{ij} = \phi_2.\alpha_{ij} \text{ if } t.\alpha_{ij} \neq \alpha_{ij}, \text{ and } \beta_{ij} = \alpha_{ij}, \text{ otherwise.}$$

The label  $ij$  on  $\beta_{ij}$  is not unique as  $\beta_{ij} = \beta_{kl}$  whenever  $\{x_i, x_j\} \triangleleft t = \{x_k, x_l\}$ . Of the two sets  $\{i, j\}$  and  $\{k, l\}$  labeling  $\beta_{ij}$  we agree to use the one with the smallest element, and call such minimal. We claim:

$$(2.12) \quad \text{The elements } \{\beta_{ij}\} \text{ form a basis of } \text{Alt}_N(G).$$

PROOF: First we note that for every group  $M$  of exponent 2  $M_N = M^{C_2}$ . Suppose  $\beta \in \text{Alt}(G)^{C_2}$ . Say  $\beta = \prod \alpha_{ij}^{e_{ij}}$ ,  $e_{ij} = 0, 1$ . From  $t.\beta = \prod (t.\alpha_{ij})^{e_{ij}} = \beta$  we see that if  $\alpha_{ij}$  occurs in  $\beta$ , i.e.  $e_{ij} = 1$ , then so does  $t.\alpha_{ij}$ , hence  $\beta$  is a product of  $\beta_{ij}$ .  $\square$

(ii) We want to show  $\underline{a}(Z_N^2(\triangleleft)) = \text{Alt}_N(G)$ . The restriction  $\underline{a}^*$  of  $\underline{a}$  to  $Z_N^2(\triangleleft)$  induces a  $C_2$ -homomorphism  $Z_N^2(\triangleleft) \xrightarrow{\underline{a}^*} \text{Alt}_N(G)$  whose kernel equals  $B^2(G, \mathbb{k}^\bullet) \cap Z_N^2(\triangleleft) =: B_N^2(\triangleleft)$ .

We begin by showing  $\phi_2.\text{Alt}(G) \subset \text{im } \underline{a}^*$ . For, if  $\beta = \phi_2.\alpha$ , pick an  $s \in Z^2(G, \mathbb{k}^\bullet)$  with  $\underline{a}(s) = \alpha$ . Then  $(t-1).s \in Z_N^2(\triangleleft)$ , and  $\underline{a}((t-1).s) = (t-1).\underline{a}(s) = (t-1).\alpha = \phi_2.\alpha$ , as  $\alpha^2 = 1$ , which gives the inclusion.

By step (i) and definition (2.11) it remains to show that all fixed points  $\alpha_{ij}$  lie in  $\text{im } \underline{a}^*$ . By formula (2.10)  $\alpha_{ij}$  is a fixed point if and only if either

$$(a) \quad \{i, j\} \subset \{2m+1, \dots, n\} \text{ or } (b) \quad \{i, j\} = \{2k-1, 2k\}$$

for some  $k$ ,  $1 \leq k \leq m$ . Below we find it convenient to write  $s_{i,j}$  for  $s_{\alpha_{ij}}$ .

Consider case (a). We claim  $s_{i,j}$  is a fixed point. For,  $t.s_{i,j}$  is bi-multiplicative, hence is determined by its values at  $(x_k, x_l)$ . It is immediate that  $t.s_{i,j}(x_k, x_l) = s_{i,j}(x_k, x_l)$  for all  $(x_k, x_l)$ , whence the assertion. Since  $s_{i,j}^2 = 1$  for all  $i, j$ ,  $\phi_2.s_{i,j} = 1$ , hence  $s_{i,j} \in Z_N^2(\triangleleft)$ . As  $\underline{a}(s_{i,j}) = \alpha_{ij}$ , this case is done.

We take up (b). Say  $z = s_{2i-1, 2i}$  for some  $i$ ,  $1 \leq i \leq m$ . An easy verification gives  $\phi_2.z = \alpha_{2i-12i} \neq 1$ . Thus  $z \notin Z_N^2(\triangleleft)$ . To prove (ii) we need to find a coboundary  $\delta g_i$  such that  $z\delta g_i \in Z_N^2(\triangleleft)$ . Since  $\underline{a}(\alpha_{2i-12i}) = 1$ ,  $\alpha_{2i-12i} = \delta f_i$  for some  $f_i : G \rightarrow \mathbb{k}^\bullet$ . Put  $G_i$  for the subgroup of  $G$  generated by all  $x_j$ ,  $j \neq 2i-1, 2i$ . We assert that one choice is the function  $f_i$  defined by

$$(2.13) \quad f_i(x_{2i-1}^{j_1} x_{2i}^{j_2} x') = (-1)^{j_1+j_2+j_1j_2} \text{ for all } x' \in G_i$$

For, on the one hand it is immediate that for any  $x', x'' \in G_i$

$$\alpha_{2i-12i}(x_{2i-1}^{j_1} x_{2i}^{j_2} x', x_{2i-1}^{k_1} x_{2i}^{k_2} x'') = (-1)^{j_1k_2+j_2k_1}$$

On the other hand the definitions of  $f_i$  and differential  $\delta$  give

$$\begin{aligned} \delta f_i(x_{2i-1}^{j_1} x_{2i}^{j_2} x', x_{2i-1}^{k_1} x_{2i}^{k_2} x'') \\ &= (-1)^{j_1+j_2+j_1j_2} (-1)^{k_1+k_2+k_1k_2} (-1)^{j_1+k_1+j_2+k_2+(j_1+k_1)(j_2+k_2)} \\ &= (-1)^{j_1k_2+j_2k_1} \end{aligned}$$

Define the function  $g_i : G \rightarrow \mathbb{k}^\bullet$  by  $g_i(x_{2i-1}^{j_1} x_{2i}^{j_2} x') = \iota^{j_1+j_2+j_1j_2}$  where  $\iota^2 = -1$ . One can check easily the equalities  $f_i^2 = 1$  and  $t.g_i = g_i$ ,  $g_i^2 = f_i$ . Hence we have  $f_i(\phi_2.g_i) = f_i g_i^2 = f_i^2 = 1$ , and then a calculation

$$\phi_2.(z\delta g_i) = (\phi_2.z)(\phi_2.\delta g_i) = \delta f_i \cdot \delta(\phi_2.g_i) = \delta(f_i(\phi_2.g_i)) = 1$$

completes the proof of (ii).

(iii) Suppose  $Z_N^2(\triangleleft) = B_N^2(\triangleleft) \times C$  where  $C$  is a  $C_2$ -invariant subgroup. Then  $C$  is mapped isomorphically on  $\text{Alt}_N(G)$  under  $\underline{a}$  and so there is a unique  $z \in C$  such that  $\underline{a}(z) = \alpha_{12}$ . Since  $\underline{a}(s_{1,2}) = \alpha_{12}$ ,  $z = s_{1,2}\delta g$  for some  $g : G \rightarrow \mathbb{k}^\bullet$ . Further, as  $\alpha_{12}$  is a fixed point  $\underline{a}(t.z) = \alpha_{12}$  as well, hence  $t.z = z$ . In addition, since  $\text{Alt}(G)$  is an elementary 2-group,  $1 = z^2 = (s_{1,2}\delta g)^2 = (\delta g)^2 = \delta(g^2)$ . It follows that  $g^2$  is a character of  $G$ . Moreover,  $t.z = z$  is equivalent to  $t.s_{1,2}(t.\delta g) = s_{1,2}\delta g$  which in turn gives  $s_{1,2}(t.s_{1,2})(t.\delta g) = \delta g$ . As  $\phi_2.s_{1,2} = \alpha_{12} = \delta f_1$

we have  $\delta f_1(t.\delta g) = \delta g$  which implies  $\delta f_1 = \delta g(t.\delta g)$  on the account of  $(\delta g)^2 = \delta(g^2) = 1$  as  $g^2$  is a character. Equivalently we have the equality

$$(2.14) \quad f_1 = g \cdot (t.g) \cdot \chi \text{ for some } \chi \in \widehat{G}.$$

Noting that  $f_1$  is defined up to a character of  $G$  we can assume that  $f_1(x_1) = 1 = f_1(x_2)$  and  $f_1(x_1x_2) = -1$ . For,  $f_1$  is defined as any function satisfying  $\delta f_1 = \alpha_{12}$ . As  $\delta(f_1\chi) = \delta f_1$  for any  $\chi \in \widehat{G}$ ,  $f_1$  can be modified by any  $\chi$ . By (2.13)  $f_1(x_j) = -1 = f_1(x_1x_2)$ ,  $j = 1, 2$  so we can take  $\chi$  such that  $\chi(x_1) = \chi(x_2) = -1$ . The equality (2.14) implies that for some  $\chi \in \widehat{G}$  there holds

$$(*) \quad 1 = f_1(x_j) = g(x_1)g(x_2)\chi(x_j), \quad j = 1, 2, \text{ and}$$

$$(**) \quad -1 = f_1(x_1x_2) = g(x_1x_2)^2\chi(x_1x_2)$$

as  $t$  swaps  $x_1$  and  $x_2$ . Since  $g^2$  is a character,  $g^2(a) = \pm 1$  for every  $a \in G$ . It follows that  $g(x_1) = \iota^m$  and  $g(x_2) = \iota^k$  for some  $0 \leq m, k \leq 3$ . Then equation  $(*)$  gives  $1 = \iota^{m+k}\chi(x_j)$ . This equality shows that  $\chi(x_1) = \chi(x_2)$  and  $m + k$  is even, because  $\chi(a) = \pm 1$  for all  $a$ . Now  $(**)$ , and the fact that  $g^2$  is a character, gives  $-1 = g^2(x_1)g^2(x_2)\chi(x_1)\chi(x_2) = \iota^{2(m+k)}\iota^{-2(m+k)} = 1$ , a contradiction. This completes the proof of the Lemma.  $\square$

Finally we prove (3). Let  $G$  be a group with a decomposition (2.9). Set  $C$  to be the subgroup of  $Z_N^2(\triangleleft)$  generated by the set  $B = B' \cup B'' \cup B'''$  where

$$B' = \{\phi_2.s_{i,j} | \alpha_{ij} \text{ is not a fixed point, and } \{i, j\} \text{ is minimal}\}$$

$$B'' = \{s_{i,j} | i < j \text{ and } \{i, j\} \subset \{2m+1, \dots, n\}\}$$

$$B''' = \{s_{2i-1,2i}\delta g_i | i = 1, \dots, m\}.$$

There  $g_i$  is chosen as in the case (ii) of Lemma 2.6. Passing on to  $Z_N^2(\triangleleft)/\ker \Phi$  we denote by  $\overline{B_N^2(\triangleleft)}$  and  $\overline{C}$  the images of these subgroups in  $Z_N^2(\triangleleft)/\ker \Phi$ . Pick a  $v \in \overline{B}$ . If  $v \in B' \cup B''$  then  $v^2 = 1$  because the corresponding  $s_{i,j}$  has order 2. For  $v = s_{2i-1,2i}\delta g_i$ ,  $v^2 = \delta g_i^2 = \delta f_i$ . We know  $t.f_i = f_i$  and  $f_i^2 = 1$  and therefore  $\phi_2.f_i = 1$ , whence  $\delta f_i \in \ker \Phi$  by definition (2.5). It follows that  $\overline{v}^2 = 1$  for all  $\overline{v} \in \overline{B}$ . Furthermore, by Lemma 2.6 the mapping  $\underline{a}$  sends  $\overline{B}$  to the basis (2.12) of  $\text{Alt}_N(G)$ . Therefore  $\overline{C}$  is isomorphic to  $\overline{\text{Alt}_N(G)}$  at least as an abelian group and forms a complement to  $\overline{B_N^2(\triangleleft)}$  in  $Z_N^2(\triangleleft)/\ker \Phi$ . Since  $\text{Alt}_N(G)$  consists of fixed points the proof will be completed if we show the same for  $\overline{C}$ . The fact that  $B' \cup B''$  consists of fixed points follows from  $t\phi_2 = \phi_2$  and part (a) of Lemma 2.6(ii). For an  $s_{2i-1,2i}\delta g_i$ , the equality

$\phi_2 \cdot s_{2i-1,2i} = \delta f_i$  gives  $t \cdot s_{2i-1,2i} = s_{2i-1,2i} \delta f_i$ . Since  $\delta f_i \in \ker \Phi$  and  $t \cdot \delta g_i = \delta g_i$  we see that  $s_{2i-1,2i} \delta g_i$  is a fixed point in  $Z_N^2(\triangleleft) / \ker \Phi$  which completes the proof.  $\square$

### 3. THE ISOMORPHISM THEOREMS

We begin with a general observation. Let  $H$  be an extension of type (A). The mapping  $\pi$  induces a  $\mathbb{k}F$ -comodule structure  $\rho_\pi$  on  $H$  via

$$(3.1) \quad \rho_\pi : H \rightarrow H \otimes \mathbb{k}F, \rho_\pi(h) = h_1 \otimes \pi(h_2).$$

$H$  becomes an  $F$ -graded algebra with the graded components  $H_f = \{h \in H \mid \rho_\pi(h) = h \otimes f\}$ . Let  $\chi : \mathbb{k}F \rightarrow H$  be a section of  $\mathbb{k}F$  in  $H$ . By definition  $\chi$  is a convolution invertible  $\mathbb{k}F$ -comodule mapping, that is

$$(3.2) \quad \rho_\pi(\chi(f)) = \chi(f) \otimes f, \text{ for every } f \in F$$

Set  $\bar{f} = \chi(f)$ . The next lemma is similar to [23, 3.4] or [24, 7.3.4].

**Lemma 3.1.** *For every  $f \in F$  there holds  $H_f = \mathbb{k}^G \bar{f}$*

PROOF: By definition of components  $H_1 = H^{\text{co}\pi}$  which equals to  $\mathbb{k}^G$  by the definition of extension. By (3.2)  $\rho_\pi(\bar{f}) = \bar{f} \otimes f$ , hence  $\mathbb{k}^G \bar{f} \subset H_f$ . Since the containment holds for all  $f$ , the equalities

$$H = \bigoplus_{f \in F} H_f = \bigoplus_{f \in F} \mathbb{k}^G \bar{f}$$

force  $H_f = \mathbb{k}^G \bar{f}$  for all  $f \in F$ .  $\square$

**Definition 3.2.** Given two  $F$ -graded algebras  $H = \bigoplus H_f$  and  $H' = \bigoplus H'_f$  and an automorphism  $\alpha : F \rightarrow F$  we say that a linear mapping  $\psi : H \rightarrow H'$  is an  $\alpha$ -graded morphism if  $\psi(H_f) = H'_{\alpha(f)}$  for all  $f \in F$ .

**Lemma 3.3.** *Suppose  $H$  and  $H'$  are two extensions of  $\mathbb{k}F$  by  $\mathbb{k}^G$  and  $\psi : H \rightarrow H'$  a Hopf isomorphism sending  $\mathbb{k}^G$  to  $\mathbb{k}^G$ . Then  $\psi$  is an  $\alpha$ -graded mapping for some  $\alpha$ .*

PROOF: Suppose  $H$  and  $H'$  are given by sequences

$$\mathbb{k}^G \xrightarrow{\iota} H \xrightarrow{\pi} \mathbb{k}F, \text{ and } \mathbb{k}^G \xrightarrow{\iota'} H' \xrightarrow{\pi'} \mathbb{k}F$$

By definition of extension  $\text{Ker } \pi = H(\mathbb{k}^G)^+$  and likewise  $\text{Ker } \pi' = H'(\mathbb{k}^G)^+$ . By assumption  $\psi(\mathbb{k}^G) = \mathbb{k}^G$ , hence  $\psi$  induces a Hopf isomorphism  $\alpha : H/H(\mathbb{k}^G)^+ \rightarrow H'/H'(\mathbb{k}^G)^+$ . Replacing  $H/H(\mathbb{k}^G)^+$  and  $H'/H'(\mathbb{k}^G)^+$  by  $\mathbb{k}F$  we can treat  $\alpha$  as a Hopf isomorphism  $\alpha : \mathbb{k}F \rightarrow$

$\mathbb{k}F$ .  $\alpha$  is in fact an automorphism of  $F$ . We arrive at a commutative diagram

$$\begin{array}{ccccc} \mathbb{k}^G & \xrightarrow{\iota} & H & \xrightarrow{\pi} & \mathbb{k}F \\ \psi \downarrow & & \psi \downarrow & & \alpha \downarrow \\ \mathbb{k}^G & \xrightarrow{\iota'} & H' & \xrightarrow{\pi'} & \mathbb{k}F \end{array}$$

Since  $\psi$  is a coalgebra mapping for every  $f \in F$  we have

$$\begin{aligned} \Delta_{H'}(\psi(\bar{f})) &= (\psi \otimes \psi)\Delta_H(\bar{f}) = \psi((\bar{f})_1) \otimes \psi((\bar{f})_2), \text{ hence} \\ \rho_{\pi'}(\psi(\bar{f})) &= \psi((\bar{f})_1) \otimes \pi'\psi((\bar{f})_2) = \psi((\bar{f})_1) \otimes \alpha\pi((\bar{f})_2) \end{aligned}$$

On the other hand, applying  $\psi \otimes \alpha$  to the equality  $\rho_{\pi}(\bar{f}) = (\bar{f})_1 \otimes \pi((\bar{f})_2) = \bar{f} \otimes f$  gives

$$\psi((\bar{f})_1) \otimes \alpha\pi((\bar{f})_2) = \psi(\bar{f}) \otimes \alpha(f)$$

whence we deduce  $\rho_{\pi'}(\psi(\bar{f})) = \psi(\bar{f}) \otimes \alpha(f)$ . Thus  $\psi(\bar{f}) \in H'_{\alpha(f)}$  which shows the inclusion

$$\psi(H_f) = \psi(\mathbb{k}^G \bar{f}) = \mathbb{k}^G \psi(\bar{f}) \subseteq H'_{\alpha(f)} = \mathbb{k}^G \overline{\alpha(f)}$$

Since both sides of the above inclusion have equal dimensions, the proof is complete.  $\square$

In what follows  $H$  is an almost abelian Hopf algebra,  $G = G(H)$ ,  $F = C_p$ , and  $p$  is small relative to  $G$ . Let  $\triangleleft$  and  $\triangleleft'$  be two actions of  $C_p$  on  $G$ . We denote  $(G, \triangleleft)$  and  $(G, \triangleleft')$  the corresponding  $C_p$ -modules and we use the notation ' $\bullet$ ' and ' $\circ$ ' for the actions of  $C_p$  on  $\mathbb{k}^G$  corresponding by (1.4) to  $\triangleleft$  and  $\triangleleft'$ , respectively. We let  $I(\triangleleft, \triangleleft')$  denote the set of all automorphisms of  $G$  intertwining actions  $\triangleleft$  and  $\triangleleft'$ , that is automorphisms  $\lambda : G \rightarrow G$  satisfying

$$(3.3) \quad (a \triangleleft x)\lambda = a\lambda \triangleleft' x, \quad a \in G, x \in C_p$$

We make every  $\lambda$  act on functions  $\tau : C_p \times G^2 \rightarrow \mathbb{k}^\bullet$  by

$$(\tau.\lambda)(x, a, b) = \tau(x, a\lambda^{-1}, b\lambda^{-1}).$$

**Lemma 3.4.** (i) *The group  $Z^2(G, (\mathbb{k}^{C_p})^\bullet)$  is invariant under the action induced by any automorphism of  $G$ ,*

(ii) *A  $C_p$ -isomorphism  $\lambda : (G, \triangleleft) \rightarrow (G, \triangleleft')$  induces  $C_p$ -isomorphisms between the groups  $Z_c^2(\triangleleft), B_c^2(\triangleleft), H_c^2(\triangleleft)$  and  $Z_c^2(\triangleleft'), B_c^2(\triangleleft'), H_c^2(\triangleleft')$ , respectively.*

PROOF: (i) is immediate.

(ii) We must check condition (1.12) for  $\tau.\lambda$  and  $\mathbb{Z}C_p$ -linearity of the induced map. First we note  $\lambda^{-1}$  is a  $C_p$ -isomorphism between  $(G, \triangleleft')$



and  $(G, \triangleleft)$ , as one can check readily. Next we verify (1.12) and  $C_p$ -linearity in a single calculation

$$\begin{aligned}
(\tau.\lambda)(xy)(a, b) &= \tau(xy, a\lambda^{-1}, b\lambda^{-1}) \\
&= \tau(x, a\lambda^{-1}, b\lambda^{-1})(x \bullet \tau(y, a\lambda^{-1}, b\lambda^{-1})) \\
&= \tau(x, a\lambda^{-1}, b\lambda^{-1})\tau(y, a\lambda^{-1} \triangleleft x, b\lambda^{-1} \triangleleft x) \\
&= \tau(x, a\lambda^{-1}, b\lambda^{-1})\tau(y, (a \triangleleft' x)\lambda^{-1}, (b \triangleleft' x)\lambda^{-1}) \\
&= (\tau.\lambda)(x)(x \circ (\tau.\lambda)(y))(a, b).
\end{aligned}$$

In the case of  $B_c^2(\triangleleft)$ , first one checks the equality

$$(\delta_G \eta).\lambda = \delta_G(\eta.\lambda) \text{ for any } \eta : C_p \times G \rightarrow \mathbb{k}^\bullet.$$

It remains to verify the condition (1.13) for  $\eta.\lambda$ . That is done similarly to the calculation in (ii).  $\square$

Let  $(G, \triangleleft)$  be a  $C_p$ -module. Recall that  $\mathbb{A}(\triangleleft)$  denotes the group of  $C_p$ -automorphisms of  $(G, \triangleleft)$ . By the above Lemma  $Z_c^2(\triangleleft)$  is an  $\mathbb{A}(\triangleleft)$ -module. Symmetrically, the group  $A_p = \text{Aut}(C_p)$  of automorphisms of  $C_p$  acts on  $\text{Map}(C_p \times G^2, \mathbb{k}^\bullet)$  via

$$\tau.\alpha(x, a, b) = \tau(\alpha(x), a, b)$$

We want to know the effect of this action on  $Z_c^2(\triangleleft)$ . Let  $(G, \triangleleft)$  be a  $C_p$ -module. For  $\alpha \in A_p$  we define a  $C_p$ -module  $(G, \triangleleft^\alpha)$  via

$$a \triangleleft^\alpha x = a \triangleleft \alpha(x), \quad a \in G, \quad x \in C_p$$

Similarly, an action ' $\bullet$ ' of  $C_p$  on  $\mathbb{k}^G$  can be twisted by  $\alpha$  into ' $\bullet^\alpha$ ' via

$$x \bullet^\alpha r = \alpha(x) \bullet r, \quad r \in \mathbb{k}^G$$

One can see easily that if  $\bullet$  and  $\triangleleft$  correspond to each other by (1.4), then so do  $\bullet^\alpha$  and  $\triangleleft^\alpha$ .

**Lemma 3.5.** (i) *If  $\lambda \in I(\triangleleft, \triangleleft')$ , then  $\lambda \in I(\triangleleft^\alpha, \triangleleft'^\alpha)$  for every  $\alpha \in A_p$ ,*

(ii) *The mapping  $\tau \mapsto \tau.\alpha$  induces an  $\mathbb{A}(\triangleleft)$ -isomorphism between  $Z_c^2(\triangleleft), B_c^2(\triangleleft), H_c^2(\triangleleft)$  and  $Z_c^2(\triangleleft^\alpha), B_c^2(\triangleleft^\alpha), H_c^2(\triangleleft^\alpha)$ , respectively for every  $\alpha \in A_p$ .*

PROOF: (i) For every  $a \in G, x \in C_p$  we have

$$(a \triangleleft^\alpha) \lambda = (a \triangleleft \alpha(x)) \lambda = a \lambda \triangleleft' \alpha(x) = a \lambda \triangleleft'^\alpha x$$

(ii) First we note that  $\mathbb{A}(\triangleleft)$  can be identified with  $\mathbb{A}(\triangleleft^\alpha)$  for any  $\alpha$  by the following calculation

$$(g \triangleleft^\alpha x) \phi = (g \triangleleft \alpha(x)) \phi = (g \phi) \triangleleft \alpha(x) = g \phi \triangleleft^\alpha x \text{ for every } \phi \in \mathbb{A}(\triangleleft).$$

Thus we will treat every  $Z_c^2(\triangleleft^\alpha)$  as an  $\mathbb{A}(\triangleleft)$ -module. Our next step is to show that for every  $\tau \in Z_c^2(\triangleleft)$ ,  $\tau.\alpha$  lies in  $Z_c^2(\triangleleft^\alpha)$ . This boils down to checking (1.12) for  $\tau.\alpha$  with the  $\triangleleft^\alpha$ -action:

$$\begin{aligned} (\tau.\alpha)(xy) &= \tau(\alpha(x)\alpha(y)) = \tau(\alpha(x))(\alpha(x) \bullet \tau(\alpha(y))) \\ &= \tau(\alpha(x))(x \bullet^\alpha \tau(\alpha(y))) = (\tau.\alpha)(x)(x \bullet^\alpha (\tau.\alpha)(y)). \end{aligned}$$

As for  $\mathbb{A}(\triangleleft)$ -linearity, for every  $\phi \in \mathbb{A}(\triangleleft)$ , we have

$$\begin{aligned} ((\tau.\alpha).\phi)(x, a, b) &= (\tau.\alpha)(x, a\phi^{-1}, b\phi^{-1}) = \tau(\alpha(x), a\phi^{-1}, b\phi^{-1}) \\ &= (\tau.\phi)(\alpha(x), a, b) = ((\tau.\phi).\alpha)(x, a, b). \end{aligned}$$

□

We need several short remarks.

**Lemma 3.6.** *Suppose  $\tau$  is a 2-cocycle. Assume  $r \in (\mathbb{k}^G)^\bullet$  is such that  $\phi_p.r = \epsilon$ . Set  $r_i = \phi_i.r$ ,  $1 \leq i \leq p$ . Define a 1-cocycle  $\zeta : C_p \rightarrow (\mathbb{k}^G)^\bullet$  by  $\zeta(t^i) = r_i$  and a 2-cocycle  $\tau' = \tau(\delta_G \zeta)$ . Then the mapping*

$$\iota : H(\tau, \triangleleft) \rightarrow H(\tau', \triangleleft), \quad \iota(p_a t^i) = p_a r_i t^i, \quad a \in G, 1 \leq i \leq p$$

*is an equivalence of extensions.*

PROOF: It suffices to show  $\delta_G \zeta \in B_c^2$  for then [23, 5.2] yields the conclusion of the lemma. Now  $\delta_G \zeta \in B_c^2$  means that  $\zeta$  satisfies (1.13). The argument of Lemma 2.2 used to derive (1.12) from the condition (2.4) works verbatim for  $\zeta$ . □

**Lemma 3.7.**  *$H(\tau, \triangleleft)$  is cocommutative iff  $\tau$  lies in  $H_{cc}^2(\triangleleft)$ .*

PROOF:  $H^*(\tau, \triangleleft)$  is commutative iff  $\bar{a}\bar{b} = \bar{b}\bar{a}$  which is equivalent to  $\tau(a, b) = \tau(b, a)$ . This condition is equivalent to  $\tau(t) : G \times G \rightarrow \mathbb{k}^\bullet$  being a symmetric 2-cocycle. Indeed, one implication is trivial, while if  $\tau(t)$  is symmetric, then as pointed out in the odd case of Proposition 2.5  $\tau(t)$  is a coboundary, that is an element of  $B_N^2 / \ker \Phi$ . A reference to Lemma 2.3(i) completes the proof. □

Unless stated otherwise,  $H(\tau, \triangleleft)$  is a noncocommutative Hopf algebra. We pick another algebra  $H(\tau', \triangleleft')$  isomorphic to  $H(\tau, \triangleleft)$  via  $\psi : H(\tau, \triangleleft) \rightarrow H(\tau', \triangleleft')$ . The next observation is noted in [18, p. 802].

**Lemma 3.8.** *Mapping  $\psi$  induces an Hopf automorphism of  $\mathbb{k}^G$ .*

□

Let  $G$  be a finite group and  $\text{Aut}_{\text{Hf}}(\mathbb{k}^G)$  be the group of Hopf automorphisms of  $\mathbb{k}^G$ . Identifying  $(\mathbb{k}^G)^*$  with  $\mathbb{k}G$  as in §1, for every  $\phi \in \text{Aut}_{\text{Hf}}(\mathbb{k}^G)$  the transpose mapping  $\phi^*$  is a Hopf automorphism of  $\mathbb{k}G$ , hence an automorphism of  $G$ . This leads up to

**Lemma 3.9.** *Let  $G$  be a finite group. The mapping  $\phi \mapsto \phi^*$  is an isomorphism between  $\text{Aut}_{\text{HF}}(\mathbb{k}^G)$  and  $\text{Aut}(G)$ .  $\phi$  is a  $C_p$ -isomorphism  $(\mathbb{k}^G, \bullet) \rightarrow (\mathbb{k}^G, \circ)$  if and only if  $\phi^*$  is a  $C_p$ -isomorphism  $(G, \triangleleft) \rightarrow (G, \triangleleft')$ .*

PROOF: The first assertion is clear by the opening remark. Next we recall that  $\phi^*$  acts on  $G$  via

$$(3.4) \quad (a\phi^*)(f) := f(a\phi^*) = \phi(f)(a), \quad f \in \mathbb{k}^G.$$

Let  $\triangleleft$  and  $\triangleleft'$  be actions related to  $\bullet$  and  $\circ$  by (1.4). The last conclusion follows from the calculation

$$\begin{aligned} ((a\triangleleft' x)\phi^*)(f) &= \phi(f)(a\triangleleft' x) = (x \circ \phi(f))(a) = \phi(x \bullet f)(a) \\ &= (a\phi^*)(x \bullet f) = (a\phi^* \triangleleft x)(f), \text{ for all } f \in \mathbb{k}^G. \end{aligned}$$

□

We proceed to the formulation of isomorphism theorems. First we rephrase definitions of  $[\triangleleft]$  and  $C(\triangleleft)$ . Let ' $\simeq$ ' denote equivalence of actions of  $C_p$  on  $G$ . With  $\mathcal{R}$  defined in the Introduction we have  $[\triangleleft] = \{\triangleleft' \in \mathcal{R} \mid \triangleleft' \simeq \triangleleft^\alpha \text{ for some } \alpha \in A_p\}$  and  $C(\triangleleft) = \{\alpha \in A_p \mid \triangleleft^\alpha \simeq \triangleleft\}$ . Furthermore we denote by  $\mathcal{G}(\triangleleft)$  the subgroup of  $\text{Aut}(G)$  generated by  $\mathbb{A}(\triangleleft)$  and a set of automorphisms  $\lambda_\alpha \in I(\triangleleft, \triangleleft^\alpha)$  one for every  $\alpha \in C(\triangleleft)$  if  $\triangleleft$  is nontrivial, and  $\mathbb{A}(\triangleleft) \times A_p$ , otherwise.

**Proposition 3.10.**  *$\mathcal{G}(\triangleleft)$  is a crossed product of  $\mathbb{A}(\triangleleft)$  with  $C(\triangleleft)$ .*

PROOF: The claim holds by definition for the trivial action. Else, we note that  $\lambda\mathbb{A}(\triangleleft)\lambda^{-1} = \mathbb{A}(\triangleleft)$  for every  $\lambda \in I(\triangleleft, \triangleleft^\alpha)$  by Lemmas 3.4(ii), 3.5(i). In addition, for every  $\lambda, \mu \in I(\triangleleft, \triangleleft^\alpha)$ ,  $\lambda^{-1}\mu \in \mathbb{A}(\triangleleft)$ . Thus we have  $I(\triangleleft, \triangleleft^\alpha) = \mathbb{A}(\triangleleft)\lambda_\alpha$ . It follows that  $\lambda_\alpha \cdot \lambda_\beta = \phi(\alpha, \beta)\lambda_{\alpha\beta}$  for some  $\phi(\alpha, \beta) \in \mathbb{A}(\triangleleft)$ . It remains to show that the kernel of  $\pi : \mathcal{G}(\triangleleft) \rightarrow C(\triangleleft)$ ,  $\pi(\phi\lambda_\alpha) = \alpha$  equals  $\mathbb{A}(\triangleleft)$ . Pick  $\alpha : x \rightarrow x^k, k \neq 1$ . Clearly  $\lambda \in I(\triangleleft, \triangleleft^\alpha)$  iff  $t\lambda = \lambda t^k$  where we treat  $t \in C_p$  as automorphism of  $G$ . Since elements of  $\mathbb{A}(\triangleleft)$  commute with  $t$ ,  $I(\triangleleft, \triangleleft^\alpha) \cap \mathbb{A}(\triangleleft) = \emptyset$ . □

Our next goal is to define a  $\mathcal{G}(\triangleleft)$ -module structure on  $H_c^2(\triangleleft)$ . As we mentioned above  $H_c^2(\triangleleft)$  is  $\mathbb{A}(\triangleleft)$ -module. Further, for every  $\lambda \in I(\triangleleft, \triangleleft^\alpha)$  Lemmas 3.4(ii), 3.5(ii) show that the mapping

$$(3.5) \quad \omega_{\lambda, \alpha} : \tau \mapsto \tau \cdot \lambda \alpha^{-1}, \quad \tau \in H_c^2(\triangleleft)$$

is an automorphism of  $H_c^2(\triangleleft)$ . We denote by  $\bar{\phi}$  the automorphism of  $H_c^2(\triangleleft)$  induced by  $\phi \in \mathbb{A}(\triangleleft)$  and we abbreviate  $\omega_{\lambda_\alpha, \alpha}$  to  $\omega_\alpha$ .

**Lemma 3.11.** *The mapping  $\phi\lambda_\alpha \mapsto \bar{\phi}\omega_\alpha, \phi \in \mathbb{A}(\triangleleft), \alpha \in C(\triangleleft)$  defines  $\mathcal{G}(\triangleleft)$ -module structure on  $H_c^2(\triangleleft)$ .*

PROOF:  $H_c^2(\triangleleft)$  is a subquotient of  $Z^2(G, (\mathbb{k}^{C_p})^\bullet)$ , and the action of  $\mathbb{A}(\triangleleft)$  and  $\omega_\alpha$  on  $H_c^2(\triangleleft)$  are induced from their action on  $Z^2(G, (\mathbb{k}^{C_p})^\bullet)$ . Furthermore it is elementary to check that every  $\lambda \in \text{Aut}(G)$  commutes with every  $\beta \in A_p$  as mappings of  $Z^2(G, (\mathbb{k}^{C_p})^\bullet)$ . It follows that the equalities  $\omega_\alpha \omega_\beta = \overline{\phi(\alpha, \beta)} \omega_{\alpha\beta}$  and  $\omega_\alpha \overline{\phi} \omega_\alpha^{-1} = \lambda_\alpha \overline{\phi} \lambda_\alpha^{-1}$  hold in  $\text{Aut}(Z^2(G, (\mathbb{k}^{C_p})^\bullet))$ . This shows that the mapping of the Lemma is a homomorphism, as needed.  $\square$

**Theorem 3.12.** (I). *Noncocommutative extensions  $H(\tau, \triangleleft)$  and  $H(\tau', \triangleleft')$  are isomorphic if and only if*

- (i) *There exist an  $\alpha \in A_p$  and a  $C_p$ -isomorphism  $\lambda : (G, \triangleleft) \rightarrow (G, \triangleleft'^\alpha)$  such that*
- (ii)  *$\tau' = \tau \cdot (\lambda \alpha^{-1})$  in  $H_c^2(\triangleleft')$ .*

(II). *There is a bijection between the orbits of  $\mathcal{G}(\triangleleft)$  in  $H_c^2(\triangleleft)$  not contained in  $H_{cc}^2(\triangleleft)$  and the isomorphism types of noncocommutative extensions in  $\text{Ext}_{[\triangleleft]}(\mathbb{k}C_p, \mathbb{k}^G)$ .*

PROOF: (I). In one direction, suppose  $\psi : H(\tau, \triangleleft) \rightarrow H(\tau', \triangleleft')$  is an isomorphism. By Lemma 3.8  $\psi$  induces an automorphism  $\phi : \mathbb{k}^G \rightarrow \mathbb{k}^G$ , and from Lemma 3.3 we have the equality  $\psi(t) = rt^k$  for some  $k$  and  $r \in \mathbb{k}^G$ . The equality  $\psi(t^p) = 1$  implies  $(rt^k)^p = \phi_p(t^k) \circ r = 1$  and, as  $\phi_p(t^k) = \phi_p(t)$ , we have  $\phi_p \circ r = 1$  which shows  $r \in (\mathbb{k}^G)^\bullet$ . Let  $\alpha : x \mapsto x^k, x \in C_p$  be this automorphism of  $C_p$ , and set  $\phi = \psi|_{\mathbb{k}^G}$ . Then the calculation

$$\phi(t \bullet f) = \psi(tft^{-1}) = r\alpha(t)\phi(f)\alpha(t)^{-1}r^{-1} = \alpha(t) \circ \phi(f), f \in \mathbb{k}^G$$

shows  $\phi : (\mathbb{k}^G, \bullet) \rightarrow (\mathbb{k}^G, \circ^\alpha)$  is a  $C_p$ -isomorphism. It follows by Lemma 3.9 that  $(G, \triangleleft'^\alpha)$  is isomorphic to  $(G, \triangleleft)$  under  $\phi^*$ , hence  $\lambda = (\phi^*)^{-1} : (G, \triangleleft) \rightarrow (G, \triangleleft'^\alpha)$  is a required isomorphism.

It remains to establish the second condition of the theorem. To this end we first modify  $\psi$ . Namely, set  $s = \phi^{-1}(r)$  and observe that, as  $\phi^{-1}$  is a  $C_p$ -mapping and  $\phi_p \circ^\alpha r = 1$ , we get  $\phi_p \bullet s = \phi^{-1}(\phi_p \circ^\alpha r) = 1$ . Therefore by Lemma 3.6 there is an equivalence  $\iota : H(\tau, \triangleleft) \rightarrow H(\tilde{\tau}, \triangleleft)$  with  $\iota(t) = st$ . Notice that  $\iota$  is an algebra map with  $\iota(s) = s$  for all  $s \in \mathbb{k}^G$ , hence  $\iota^{-1}(t) = s^{-1}t$ . Thus we have  $(\psi\iota^{-1})(t) = t^k$  by the choice of  $s$ . It follows we can assume  $\psi(t) = t^k$  hence  $\psi(x) = x^k$  for all  $x \in C_p$ .

Abbreviating  $H(\tau, \triangleleft), H(\tau', \triangleleft')$  to  $H, H'$ , respectively, we take up the identity.

$$\Delta_{H'}(\psi(x)) = (\psi \otimes \psi)\Delta_H(x), x \in C_p,$$

expressing comultiplicativity of  $\psi$  on elements of  $C_p$ . By (1.8) this translates into

$$(3.6) \quad \sum_{a,b} \tau'(x^k, a, b) p_a x^k \otimes p_b x^k = \sum_{c,d} \tau(x, c, d) \phi(p_c) x^k \otimes \phi(p_d) x^k.$$

Next we connect  $\phi(p_b)$  to the action of  $\phi^*$ . This is given by the formula

$$(3.7) \quad \phi(p_b) = p_{b(\phi^*)^{-1}}.$$

For, since  $\phi$  is an algebra map,  $\phi(p_b) = p_c$  where  $c$  is such that  $\phi(p_b)(c) = 1$ . By definition of action  $\phi^*$ ,  $\phi(p_b)(c) = (c\phi^*)(p_b) = p_b(c\phi^*)$ , hence  $c\phi^* = b$ , whence  $c = b(\phi^*)^{-1}$ .

Switching summation symbols  $c, d$  to  $l = c(\phi^*)^{-1}$  and  $m = d(\phi^*)^{-1}$ , the right-hand side of (3.6) takes on the form

$$\sum_{l,m} \tau(x, l\phi^*, m\phi^*) p_l x^k \otimes p_m x^k$$

Thus  $\psi$  is comultiplicative on  $C_p$  iff

$$(3.8) \quad \tau'(\alpha(x), a, b) = \tau(x, a\phi^*, b\phi^*) = \tau(\phi^*)^{-1}(x, a, b) = \tau.\lambda(x, a, b).$$

Applying  $\alpha^{-1}$  to the last displayed equation we arrive at

$$(3.9) \quad \tau'(x, a, b) = \tau.\lambda\alpha^{-1}(x, a, b).$$

as needed.

Conversely, let us assume hypotheses of part (I). Using Lemma 3.9 we infer that  $\lambda^{-1}$  induces a Hopf  $C_p$ -isomorphism  $\phi = (\lambda^{-1})^* : (\mathbb{k}^G, \bullet) \rightarrow (\mathbb{k}^G, \circ^\alpha)$ . We define

$$\psi : H(\tau, \triangleleft) \rightarrow H(\tau', \triangleleft') \text{ via } \psi(fx) = \phi(f)\alpha(x), f \in \mathbb{k}^G, x \in C_p.$$

First we verify that  $\psi$  is an algebra map utilizing  $\phi(x \bullet f) = \alpha(x) \circ \phi(f)$ , namely

$$\begin{aligned} \psi((fx)(f'x')) &= \psi(f(x \bullet f')xx') = \phi(f)\phi(x \bullet f')\alpha(x)\alpha(x') \\ &= \phi(f)(\alpha(x) \circ \phi(f'))\alpha(x)\alpha(x') = \phi(f)\alpha(x)\phi(f')\alpha^{-1}(x)\alpha(x)\alpha(x') \\ &= (\phi(f)\alpha(x))(\phi(f')\alpha(x')) = \psi(fx)\psi(f'x'). \end{aligned}$$

To see comultiplicativity of  $\psi$  we need to verify

$$(3.10) \quad \Delta_{H'}(\psi(fx)) = (\psi \otimes \psi)\Delta_H(fx).$$

By the multiplicativity of  $\Delta_{H'}, \psi, \Delta_H$  it suffices to check (3.10) separately for any  $f$  and for every  $x$ . Now the first case holds as  $\phi$  is a coalgebra mapping, and the second follows from  $\tau' = \tau.\lambda\alpha^{-1}$  by calculations (3.6) and (3.9).

(II). Let  $\mathcal{H}$  denote the set of all pairs  $(\tau', \triangleleft')$  with  $\triangleleft'$  and  $\tau'$  running over  $[\triangleleft]$  and  $H_c^2(\triangleleft') \setminus H_{cc}^2(\triangleleft')$ , respectively. We define an equivalence relation on  $\mathcal{H}$  by

$$(\tau', \triangleleft') \sim (\tau'', \triangleleft'') \text{ iff } H(\tau', \triangleleft') \simeq H(\tau'', \triangleleft'').$$

Let  $\mathcal{H}/\sim$  stand for the set of equivalence classes. By construction  $\mathcal{H}/\sim$  is just a copy of  ${}_{nc}\text{Ext}_{[\triangleleft]}(\mathbb{k}C_p, \mathbb{k}^G)/\cong$ . We select the subset  $\mathcal{H}(\triangleleft) = \{(\tau, \triangleleft) | \tau \in H_c^2(\triangleleft)\}$  of  $\mathcal{H}$  and define the orbit  $(\tau, \triangleleft)\mathcal{G}(\triangleleft)$  as the set  $\{(\tau', \triangleleft) | \tau' \in \tau\mathcal{G}(\triangleleft)\}$ . The proof will be complete if we show that the set  $\{C \cap \mathcal{H}(\triangleleft) | C \in \mathcal{H}/\sim\}$  coincides with the set of orbits of  $\mathcal{G}(\triangleleft)$  in  $\mathcal{H}(\triangleleft)$ . Now pick  $(\tau', \triangleleft') \in C$ . Since  $\triangleleft' \in [\triangleleft]$ , there exists an isomorphism  $\mu \in I(\triangleleft', \triangleleft^\alpha)$  hence setting  $\tau = \tau' \cdot \mu\alpha^{-1}$  we have  $(\tau, \triangleleft) \in C$  by part (I). Moreover  $C \cap \mathcal{H}(\triangleleft) \ni (\sigma, \triangleleft)$  if and only if  $H(\tau, \triangleleft) \simeq H(\sigma, \triangleleft)$ , hence by part (I) again we have  $\sigma = \tau \cdot \omega_{\lambda, \alpha}$ , that is  $\sigma \in \tau\mathcal{G}(\triangleleft)$ . Same argument shows that the equivalence class generated by  $(\tau, \triangleleft)$  intersect  $\mathcal{H}(\triangleleft)$  in the orbit of  $(\tau, \triangleleft)$ .  $\square$

**Corollary 3.13.** *For every  $\tau \in H_c^2(\triangleleft)$  the cardinality of the orbit  $\tau\mathcal{G}(\triangleleft)$  satisfies*

$$|\tau\mathbb{A}(\triangleleft)| \leq |\tau\mathcal{G}(\triangleleft)| \leq |C(\triangleleft)| |\tau\mathbb{A}(\triangleleft)|.$$

PROOF: Since  $\mathbb{A}(\triangleleft) \subseteq \mathcal{G}(\triangleleft)$  the lower bound is clear. By Proposition 3.10  $\mathcal{G}(\triangleleft) = \bigcup_{\alpha \in C(\triangleleft)} \omega_\alpha \mathbb{A}(\triangleleft)$  hence  $\tau\mathcal{G}(\triangleleft) = \bigcup_{\alpha \in C(\triangleleft)} \tau\omega_\alpha \mathbb{A}(\triangleleft)$ . It remains to note that for every  $\alpha$  the cardinality of  $\tau\omega_\alpha \mathbb{A}(\triangleleft)$  coincides with that of  $\tau\mathbb{A}(\triangleleft)$ .  $\square$

With some extra effort we can extend the bijection theorem to the entire set  $\text{Ext}_{[\triangleleft]}(\mathbb{k}C_p, \mathbb{k}^G)$  provided  $G$  is an elementary  $p$ -group for any  $p$ . Since our prime interest lies with nontrivial Hopf algebras we state the result without proof.

**Theorem 3.14.** *Let  $G$  be a finite elementary  $p$ -group. The number of isotypes of cocommutative Hopf algebras in  $\text{Ext}_{[\triangleleft]}(\mathbb{k}C_p, \mathbb{k}^G)$  equals to the number of orbits of  $\mathbb{A}(\triangleleft)$  in  $H_{cc}^2(\triangleleft)$ .*

$\square$

We comment briefly on the dual case of commutative Hopf algebras. First,  $\text{Ext}_{[\triangleleft]}(\mathbb{k}C_p, \mathbb{k}^G)$  contains a commutative Hopf algebra iff  $\triangleleft = \text{triv}$ . Second, we introduce the group  $\text{Cext}(G, C_p)$  of central extensions of  $G$  by  $C_p$  [2]. We outline properties of  $\text{Ext}_{[\text{triv}]}(\mathbb{k}C_p, \mathbb{k}^G)$  again without proof.

**Theorem 3.15.** (1) *The group  $\text{Ext}_{[\text{triv}]}(\mathbb{k}C_p, \mathbb{k}^G)$  is isomorphic to the group  $\text{Cext}(G, C_p)$  under the map  $H(\tau, \text{triv}) \mapsto \mathbb{k}^{L(\tau)}$  where  $L(\tau)$  is the central extension defined by the 2-cocycle  $\tau$ .*

(2) For  $G$  elementary  $p$ -group of rank  $n$  with an odd  $p$  the number of isotypes in  $\text{Ext}_{[\text{triv}]}(\mathbb{k}C_p, \mathbb{k}^G)$  equals  $\lfloor \frac{3n+2}{2} \rfloor$ .

For calculation of orbits of  $\mathcal{G}(\triangleleft)$  in  $H_c^2(\triangleleft)$  we prefer to use its isomorphic copy  $Z_N^2(\triangleleft)/\ker \Phi$  which we denote by  $\mathbb{X}(\triangleleft)$  and refer to it as the classifying group for  $\text{Ext}_{[\triangleleft]}(\mathbb{k}C_p, \mathbb{k}^G)$ .

We turn  $\mathbb{X}(\triangleleft)$  into a  $\mathcal{G}(\triangleleft)$ -module by transferring its action from  $Z_c^2(\triangleleft)$  to  $Z_N^2(\triangleleft)$  along  $\Theta$ . Pick some  $\omega_{\lambda, \alpha}$  and suppose  $\alpha^{-1} : x \mapsto x^l, x \in C_p$ . For  $s \in Z_N^2(\triangleleft)$  we put

$$(3.11) \quad s.\omega_{\lambda, \alpha} = (\phi_l \bullet s).\lambda.$$

**Lemma 3.16.** (i) For every prime and any action ' $\triangleleft$ ' the isomorphism  $\Theta_* : H_c^2(\triangleleft) \simeq \mathbb{X}(\triangleleft)$  of Corollary 2.4 is  $\mathcal{G}(\triangleleft)$ -linear.

(ii) For every prime and any action  $\mathbb{X}(\triangleleft)$  fits into the exact sequence

$$(3.12) \quad \widehat{G}^{C_p}/N(\widehat{G}) \twoheadrightarrow \mathbb{X}(\triangleleft) \twoheadrightarrow \underline{a}(Z_N^2(\triangleleft)).$$

(iii) For every odd  $p$  there is a  $\mathcal{G}(\triangleleft)$  splitting

$$(3.13) \quad \mathbb{X}(\triangleleft) \simeq \widehat{G}^{C_p}/N(\widehat{G}) \times \text{Alt}_N(G).$$

PROOF: (i) We begin by noting that for every  $\lambda \in I(\triangleleft, \triangleleft^\alpha)$  there holds (\*)  $x \bullet^\alpha (s.\lambda) = (x \bullet s).\lambda, x \in C_p$ . Still assuming  $\alpha^{-1} : x \rightarrow x^l$ , the conclusion (i) follows from (2.2) and the opening remark by the calculation

$$\begin{aligned} \Theta(\tau.\omega_{\lambda, \alpha}) &= (\tau.\omega_{\lambda, \alpha})(t) = (\tau.\lambda)(t^l) = (\text{by (2.2)}) \phi_l \bullet^\alpha (\tau.\lambda)(t) \\ &= \phi_l \bullet^\alpha (\tau(t).\lambda) = (\text{by (*)}) (\phi_l \bullet \tau(t)).\lambda = \Theta(\tau).\omega_{\lambda, \alpha} \end{aligned}$$

This equation demonstrates that definition (3.11) turns  $Z_N^2(\triangleleft)$  into a  $\mathcal{G}(\triangleleft)$ -module. It is immediate that  $B_c^2(\triangleleft)$  is a  $\mathcal{G}(\triangleleft)$ -subgroup of  $Z_c^2(\triangleleft)$ . By Lemma 2.3(ii)  $\ker \Phi$  is a  $\mathcal{G}(\triangleleft)$ -subgroup, which proves part (i).

(ii) The mapping  $\underline{a} : Z^2(G, \mathbb{k}^\bullet) \rightarrow \text{Alt}(G)$  of Proposition 2.5 restricted to  $Z_N^2(\triangleleft)$  gives rise to an exact sequence  $B_N^2(\triangleleft) \rightarrow Z_N^2(\triangleleft) \rightarrow \underline{a}(Z_N^2(\triangleleft))$ . Thanks to the  $\mathcal{G}(\triangleleft)$ -isomorphism  $\widehat{G}^{C_p}/N(\widehat{G}) \simeq B_N^2(\triangleleft)/\ker \Phi$  induced by  $\Phi$  (see Lemma 2.3) we arrive at the exact sequence (3.12) of  $\mathcal{G}(\triangleleft)$ -modules.

(iii) For an odd  $p$  splitting (2.8) is carried out by the mapping  $s \mapsto s\underline{a}(s^{-2}) \times \underline{a}(s^2)$  which is clearly a  $\mathcal{G}(\triangleleft)$ -map. It remains to note that homomorphism  $\Phi$  is also a  $\mathcal{G}(\triangleleft)$ -map.  $\square$

We point out that part (ii) fails in general for 2-groups.<sup>3</sup>

<sup>3</sup>See Appendix 2

#### 4. ALMOST ABELIAN HOPF ALGEBRAS OF DIMENSION $\leq p^4$

**4.1. Hopf algebras of dimension  $\leq p^3$ .** We begin by revisiting classification of semisimple Hopf algebras of dimension  $p^2, p^3$  due to [20, 18]. If  $\dim H = p^2$ , then by a Kac-Masuoka theorem [9, 20]  $H$  contains a central subHopf algebra  $\mathbb{k}C_p$  hence  $H \in \text{Ext}_{[\text{triv}]}(\mathbb{k}C_p, \mathbb{k}^{C_p})$ . Thus  $H$  is commutative, and as  $\text{Alt}(C_p) = 1$ ,  $H$  is cocommutative. It follows that  $H = \mathbb{k}L$  where  $L$  is a group of order  $p^2$ , that is  $L = C_{p^2}$  or  $C_p \times C_p$ .

Suppose  $\dim H = p^3$ . By the Kac-Masuoka theorem, loc.cit, applied to  $H^*$  we have that  $H^*$  is a central extension of the form  $\mathbb{k}C_p \hookrightarrow H^* \twoheadrightarrow Q$  where  $\dim Q = p^2$ . By the foregoing  $Q = \mathbb{k}G$  with  $G = C_{p^2}$  or  $C_p \times C_p$ . By duality  $H$  is a cocentral extension of  $\mathbb{k}C_p$  by  $\mathbb{k}^G$ . If  $G = C_{p^2}$ , then  $\text{Alt}(G) = 1$ , hence  $H$  is cocommutative. It follows that a nontrivial  $H$  belongs to  $\text{Ext}(\mathbb{k}C_p, \mathbb{k}^{C_p \times C_p})$  with a nontrivial action of  $C_p$  on  $C_p \times C_p$ .

Before moving on we introduce algebras  $R_i = \mathbb{Z}_p C_p / \langle (t-1)^i \rangle$ ,  $0 \leq i \leq p-1$  and make a notational change. Below we write  $\alpha_k$  for the mapping  $x \mapsto x^k$ ,  $x \in C_p$ ,  $\triangleleft^k$  for  $\triangleleft^{\alpha_k}$  and  $\omega_k$  for  $\omega_{\alpha_k}$ . The arguments in the next proposition will be used throughout §4.2.2.

**Proposition 4.1.** ([18]) *There are up to isomorphism  $p+7$  Hopf algebras in  $\text{Ext}(\mathbb{k}C_p, \mathbb{k}^{C_p \times C_p})$ ,  $p+1$  of which are nontrivial.*

PROOF: We run the procedure for computing the number of isoclasses for  $G = C_p \times C_p$ . Let  $\triangleleft_r$  denote the right regular action of  $C_p$  on  $R_2$ . Every nontrivial  $C_p$ -module  $(C_p \times C_p, \triangleleft)$  is isomorphic to  $(R_2, \triangleleft_r)$ . In consequence  $\text{Ext}(\mathbb{k}C_p, \mathbb{k}^G) = \text{Ext}_{[\triangleleft_r]}(\mathbb{k}C_p, \mathbb{k}^G) \cup \text{Ext}_{[\text{triv}]}(\mathbb{k}C_p, \mathbb{k}^G)$ . By Theorem 3.15(2)  $\text{Ext}_{[\text{triv}]}(\mathbb{k}C_p, \mathbb{k}^G)$  contributes four nonisomorphic algebras. It remains to show that  $\text{Ext}_{[\triangleleft_r]}(\mathbb{k}C_p, \mathbb{k}^G)$  contains  $p+3$  isotypes. To simplify notation we put  $\triangleleft = \triangleleft_r$ .

(i) The classifying group  $\mathbb{X}(\triangleleft)$ . Set  $G = R_2$  and let  $e = \bar{1}$ ,  $f = \overline{t-1}$  where  $\bar{r}$  is the image of  $r \in R_0$  in  $R_2$ . The matrix of  $t$  in the basis  $\{e, f\}$  is  $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ . Let  $\{e^*, f^*\}$  be the dual basis for  $\widehat{G}$ . The

mapping induced by  $t$  in  $\widehat{G}$  has the matrix  $T^{\text{tr}}$  relative to the dual basis. Hence  $e^*$  is fixed by  $t$  and  $N(\widehat{G}) = (t-1)^{p-1} \cdot \widehat{G} = 0$ , as  $p > 2$ , in the additive notation. It follows that  $\widehat{G}^{C_p} / N(\widehat{G}) = \langle e^* \rangle$ . Further  $\text{Alt}(G) = \widehat{G} \wedge \widehat{G}$ , where  $\wedge$  denote the multiplication in the Grassman algebra over  $\widehat{G}$ , is generated by  $e^* \wedge f^*$ , and the latter is a fixed by  $t$ . Therefore  $\phi_p(t) \cdot e^* \wedge f^* = p(e^* \wedge f^*) = 0$ , hence  $\text{Alt}_N(G) = \text{Alt}(G)$ . All in all we arrive at the equality

$$\mathbb{X}(\triangleleft) = \langle e^*, e^* \wedge f^* \rangle$$



(ii) Groups  $\mathbb{A}(\triangleleft), C(\triangleleft)$  and  $\mathcal{G}(\triangleleft)$ . By definition  $\phi \in \mathbb{A}(\triangleleft)$  iff the matrix  $\Phi$  of  $\phi$  satisfies  $\Phi T = T\Phi$  and  $\det \Phi \neq 0$ . This condition is equivalent to  $\Phi = \begin{pmatrix} c & d \\ 0 & c \end{pmatrix}, c \in \mathbb{Z}_p^\bullet$ . By the opening remark  $C(\triangleleft) = \mathbb{Z}_p^\bullet$  as  $(G, \triangleleft^k) \simeq (G, \triangleleft)$  for every  $k \in \mathbb{Z}_p^\bullet$ .

The group  $\mathcal{G}(\triangleleft)$  is generated by  $\mathbb{A}(\triangleleft)$  and a set  $\{\lambda_k | k \in \mathbb{Z}_p^\bullet\}$  with  $\lambda_k \in I(\triangleleft, \triangleleft^k)$ . An easy verification gives that  $\lambda_k$  defined via  $e.\lambda_k = e, f.\lambda_k = kf$  lies in  $I(\triangleleft, \triangleleft^k)$ .

(iii) Orbits of  $\mathcal{G}(\triangleleft)$  in  $\mathbb{X}(\triangleleft)$ . First we determine the orbits of  $\mathbb{A}(\triangleleft)$ . Pick  $\phi \in \mathbb{A}(\triangleleft)$  and suppose it has the matrix  $\Phi$  relative to  $\{e, f\}$ . It is an elementary fact that the mapping induced by  $\phi$  in  $\widehat{G}$  has the matrix  $\Phi^{\text{tr}}$  in the dual basis. If  $\Phi$  is written as in (ii) then we have

$$e^*.\phi^{-1} = ce^*, \text{ and } e^* \wedge f^*.\phi^{-1} = c^2 e^* \wedge f^*.$$

Let us identify  $ae^* + be^* \wedge f^* \in \mathbb{X}(\triangleleft)$  with the vector  $(a, b) \in \mathbb{Z}_p^2$ . By the above  $\phi \in \mathbb{A}(\triangleleft)$  acts in  $\mathbb{Z}_p^2$  via  $(a, b).\phi^{-1} = (ca, c^2b)$ .

By Corollary 3.13 the  $\mathcal{G}(\triangleleft)$ -orbit of  $(a, b)$  is the union of  $\mathbb{A}(\triangleleft)$ -orbits of elements  $(a, b).\omega_k, k \in C(\triangleleft)$ . There  $\omega_k = \lambda_k \alpha_k^{-1}$ , and for every  $x \in \mathbb{X}(\triangleleft)$  there holds by (3.11)  $x.\omega_k = (\phi_l.x).\lambda_k$  where  $l = k^{-1}$ . Since  $e^*$  and  $e^* \wedge f^*$  are fixed by  $t$  we have  $\phi_l.x = lx$  for  $x = e^*, e^* \wedge f^*$ . Moreover it is immediate that  $e.\lambda_k = e^*$  and  $e^* \wedge f^*.\lambda_k = le^* \wedge f^*$ . We conclude that  $(a, b).\omega_k = (la, l^2b) \in (a, b)\mathbb{A}(\triangleleft)$ . It follows that  $\mathcal{G}(\triangleleft)$ -orbits coincide with  $\mathbb{A}(\triangleleft)$ -orbits. We compute the latter.

The subset  $\mathbb{Z}_p^{\bullet 2}$  of  $\mathbb{Z}_p^2$  is stable under action of  $\mathbb{A}(\triangleleft)$ . For every  $m \in \mathbb{Z}_p^\bullet$  the set  $(1, m)\mathbb{A}(\triangleleft)$  has  $p - 1$  elements and moreover  $(1, m)\mathbb{A}(\triangleleft) \cap (1, n)\mathbb{A}(\triangleleft) = \emptyset$  if  $m \neq n$ . Since  $|\mathbb{Z}_p^{\bullet 2}| = (p - 1)^2$  the family  $\{(1, m)\mathbb{A}(\triangleleft) | m \in \mathbb{Z}_p^\bullet\}$  accounts for all orbits in  $\mathbb{Z}_p^{\bullet 2}$ . Thus we obtained  $p - 1$  nontrivial orbits. The complement  $\mathbb{Z}_p^2 \setminus \mathbb{Z}_p^{\bullet 2}$  is the union of  $\{(0, b) | b \in \mathbb{Z}_p^\bullet\}$  and  $\{(a, 0) | a \in \mathbb{Z}_p\}$ . Let  $\zeta$  be a generator of  $\mathbb{Z}_p^\bullet$ . It follows readily that  $\{(0, b) | b \in \mathbb{Z}_p^\bullet\}$  is the union of  $(0, 1)\mathbb{A}(\triangleleft)$  and  $(0, \zeta)\mathbb{A}(\triangleleft)$  which supplies two more nontrivial orbits. The second set is the union of two trivial orbits, viz.  $\{(0, 0)\}$  and its complement.  $\square$

To recover the full strength of [18] we would need to show that every  $H(\tau, \triangleleft)$  is self-dual. However, such a theorem is unattainable due to the next

**Remark 4.2.** Let  $\tau(t) = e^* \wedge f^*$  and  $H(\tau, \triangleleft)$  be the corresponding Hopf algebra.  $H(\tau, \triangleleft)^* \simeq H(\tau, \triangleleft)$  if and only if  $\frac{p-1}{2}$  is a square in  $\mathbb{Z}_p^\bullet$ .

PROOF: By general theory  $H(\tau, \triangleleft)^* \simeq H(\tau', \triangleleft)$  for some  $\tau' \in H_c^2(\triangleleft)$ . An isomorphism  $H(\tau, \triangleleft)^* \simeq H(\tau, \triangleleft)$  exists if and only if  $\tau'(t)$  and  $\tau(t)$  lie on the same orbit. The 2-cocycle  $\tau'$  is the multiplication cocycle for  $H(\tau, \triangleleft)$

written as an element of  $\text{Ext}(\mathbb{k}G, \mathbb{k}^{C_p})$ . Since  $H(\tau, \triangleleft) = \mathbb{k}(\widehat{G} \rtimes C_p)$  and  $e^*$  is a fixed point under the action of  $C_p$ ,  $\mathbb{k}\langle e^* \rangle$  is a normal subHopf algebra of  $H(\tau, \triangleleft)$  giving rise to an exact sequence

$$(4.1) \quad \mathbb{k}\langle e^* \rangle \hookrightarrow H(\tau, \triangleleft) \xrightarrow{\Pi} \mathbb{k}\overline{G}$$

where  $\overline{G} = \langle x, y \rangle$  with  $x = \Pi(f^*), y = \Pi(t)$ . Clearly  $xy = yx$  so that  $\overline{G} = G$ . Let  $\rho_\Pi = (\text{id} \otimes \Pi)\Delta_H : H(\tau, \triangleleft) \rightarrow H(\tau, \triangleleft) \otimes \mathbb{k}\overline{G}$  be the coaction induced by  $\Pi$ . We want to find a section  $\gamma : \mathbb{k}\overline{G} \rightarrow H(\tau, \triangleleft)$  splitting (4.1). This is the matter of finding  $T$  satisfying  $\rho_\Pi(T) = T \otimes y$ . It is not hard to see that  $T$  must be of the form  $ut$  for some unit  $u \in \mathbb{k}^G$  in fact a tedious but straightforward verification shows that for  $u = \sum_{i,j} \zeta^{-ij} p_{e^i f^j}$   $T = ut$  is a desired element. Since  $f^*$  is a group-like element of  $H(\tau, \triangleleft)$ ,  $\rho_\Pi(f^{*i} T^j) = f^{*i} T^j \otimes x^i y^j$ , and therefore  $\gamma : x^i y^j \mapsto f^{*i} T^j$  defines a section of  $\mathbb{k}\overline{G}$  in  $H(\tau, \triangleleft)$ . Let  $\tau' : \overline{G} \times \overline{G} \rightarrow \mathbb{k}\langle e^* \rangle$  be the 2-cocycle associated to  $\gamma$ . By definition  $\tau'(a, b) = \gamma(a)\gamma(b)\gamma(ab)^{-1}$ . We will write below  $a = x^i y^j, b = x^k y^l$ . A simple calculation using  $Tf^* = f^* e^* T$  gives  $\tau'(a, b) = e^{*jl}$ . Viewing  $e^*$  as the functional  $e^*(t^k) = \zeta^k$  on  $C_p(t)$  we conclude that  $\tau'(t, a, b) = \zeta^{jl}$ .

We need to find a decomposition of  $\tau'(t)$  according to (2.8), that is  $\tau'(t) = \underline{b} \cdot \lambda$  with  $\underline{b} \in B_N^2(\triangleleft)$  and  $\lambda \in \text{Alt}_N(G)$ . Set  $\beta = \underline{a}(\tau'(t))$  and note that by the definition of  $\underline{a}$ ,  $\beta(a, b) = \tau'(t, a, b)\tau'(t, b, a)^{-1}$  which gives  $\beta(a, b) = \zeta^{jk-il}$ . Observe that  $\beta = \underline{a}(\lambda) = \lambda^2$ , hence  $\lambda = \beta^{\frac{1}{2}}$  and therefore  $\underline{b} = \tau' \beta^{-\frac{1}{2}}$ . It follows that  $\underline{b}(a, b) = (\zeta^{\frac{1}{2}})^{jk+il}$ . Let us select  $f : \overline{G} \rightarrow \mathbb{k}^\bullet$ ,  $f(x^i y^j) = (\zeta^{-\frac{1}{2}})^{ij}$ . A straightforward calculation produces the equality  $\delta f(a, b) = \underline{b}$ . We want to find the image of  $\underline{b}$  in  $\mathbb{X}(\triangleleft)$  under  $\Phi$ , that is  $\Phi(\underline{b}) = \phi_p(t).t$ . Since  $\phi_p(t).f(a) = \prod_{i=0}^{p-1} f(a^i \triangleleft t^i)$ ,  $\phi_p(t).f(x) = 1$  as  $x \triangleleft t = x$ , and  $\phi_p(t).f(y) = \prod_{i=0}^{p-1} f(a^i b) = \prod_{i=0}^{p-1} (\zeta^{-\frac{1}{2}})^i = 1$ . Since  $\phi_p(t).f$  is a character of  $\overline{G}$ ,  $\phi_p(t).f = 1$ . Thus  $\underline{b} \in \ker \Phi$  which means  $\tau'(t) = \beta^{\frac{1}{2}}$  in  $\mathbb{X}(\triangleleft)$ . But  $\beta = \tau^{-1}$  as  $\tau(a, b) = (e^* \wedge f^*)(a, b) = \zeta^{il-jk}$ . Thus  $\tau'(t) = \tau(t)^{\frac{p-1}{2}}$  or  $(\frac{p-1}{2})e^* \wedge f^*$  in the additive notation. By Proposition 4.1(iii)  $\tau'(t)$  lies on the orbit of  $\tau(t)$  iff  $\frac{p-1}{2}$  is a square.  $\square$

**4.2. Hopf algebras of dimension  $p^4$ .** . From now on we assume that  $H$  is of dimension  $p^4$  with an abelian group  $G$  of grouplikes of order  $p^3$ .

**Theorem 4.3.** *There are  $5p + 23$  distinct nontrivial almost abelian Hopf algebras of dimension  $p^4$  if  $p > 3$ , 31 if  $p = 3, e \geq 3$  and 33, otherwise.*

**PROOF:** This will be carried out in steps. In the additive notation  $G = \mathbb{Z}_p^3$  or  $G = \mathbb{Z}_{p^2} \oplus \mathbb{Z}_p$ , and the theory splits into two parts.

4.2.1.  $G = \mathbb{Z}_p^3$ .

There are up to isomorphism two nontrivial  $\mathbb{Z}_p C_p$ -module structures on  $G$ . Namely, if  $C_p$ -module  $G$  is decomposable, then  $G \simeq R_2 \oplus R_1$ , and  $G \simeq R_3$ , otherwise.

(I) Suppose  $G \simeq R_2 \oplus R_1$ , and let  $\triangleleft_d$  be the action of  $C_p$  on  $G$  composed of regular actions of  $C_p$  on  $R_2$  and  $R_1$ . We aim to prove

**Theorem 4.4.**  $\text{Ext}_{[\triangleleft_d]}(\mathbb{k}C_p, \mathbb{k}^{C_p^3})$  contains  $2p+11$  isotypes of extensions  $2p+8$  of which are nontrivial.

PROOF: We carry out the procedure for computing the number of isotypes for  $C_p$ -module  $(G, \triangleleft_d)$ . To simplify notation we put  $\triangleleft = \triangleleft_d$ .

(1) The classifying group  $\mathbb{X}(\triangleleft)$ . Select a basis  $\{e, g, f\}$  for  $G$  where  $\{e, f\}$  is the basis for  $R_2$  as in Proposition 4.1, and  $R_1 = \mathbb{Z}_p g$ . Clearly

the matrix  $T$  of  $t$  in that basis is  $T = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ . Let  $\{e^*, g^*, f^*\}$  be

the dual basis for  $\widehat{G}$ . We fix a basis  $\{e^* \wedge g^*, e^* \wedge f^*, g^* \wedge f^*\}$  for  $\widehat{G} \wedge \widehat{G}$ . We refer to the above bases as standard.

**Proposition 4.5.**  $\mathbb{X}(\triangleleft) = \langle e^*, g^* \rangle \oplus \widehat{G} \wedge \widehat{G}$ .

PROOF: Recall  $\mathbb{X}(\triangleleft) = \widehat{G}^{C_p} / N(\widehat{G}) \oplus \text{Alt}_N(G)$ . We use the well known identification  $\text{Alt}(G) = \widehat{G} \wedge \widehat{G}$ . One can see easily that the matrix of  $t$  in the standard basis of  $\widehat{G}$  is  $T^{\text{tr}}$ . By general principles [4, III,8.5] the

matrix of  $t$  in the standard basis of  $\widehat{G} \wedge \widehat{G}$  is  $T^{\text{tr}} \wedge T^{\text{tr}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix}$ .

It follows that  $(t-1)^{p-1} \bullet \widehat{G} = 0$  and  $(t-1)^{p-1} \bullet \widehat{G} \wedge \widehat{G} = 0$ , that is  $N(\widehat{G}) = 0$  and  $(\widehat{G} \wedge \widehat{G})_N = \widehat{G} \wedge \widehat{G}$ . Further, one can see easily  $\widehat{G}^{C_p} = \langle e^*, g^* \rangle$ .  $\square$

(2) Groups  $\mathbb{A}(\triangleleft)$ ,  $C(\triangleleft)$  and  $\mathcal{G}(\triangleleft)$ . By definition  $\phi \in \mathbb{A}(\triangleleft)$  iff its matrix  $\Phi$  satisfies  $\Phi T = T \Phi$  and  $\det \Phi \neq 0$ . By a straightforward calculation one can see that  $\phi \in \mathbb{A}(\triangleleft)$  iff

$$(4.2) \quad \Phi = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & 0 & a_{11} \end{pmatrix}, \quad a_{ij} \in \mathbb{Z}_p, \quad a_{11}a_{22} \neq 0$$

It is easy to see that  $(G, \triangleleft^k) \simeq (G, \triangleleft)$  for every  $k \in \mathbb{Z}_p^\bullet$  which gives  $C(\triangleleft) = \mathbb{Z}_p^\bullet$ . Likewise one can check directly that  $\lambda_k : e \mapsto e, g \mapsto g, f \mapsto kf$  lies in  $I(\triangleleft, \triangleleft^k)$  for every  $k \in \mathbb{Z}_p^\bullet$ . This determines  $\mathcal{G}(\triangleleft)$  as the latter is generated by  $\mathbb{A}(\triangleleft)$  and the  $\lambda_k$ .

(3) Orbits of  $\mathbb{A}(\triangleleft)$  in  $\mathbb{X}(\triangleleft)$ . In order to simplify notation we change coordinates of matrices (4.2) by setting  $u = a_{11}, v = a_{22}, a_{12} = u^{-1}q, a_{23} = u^{-1}r, a_{13} = s$ . We treat the tuple  $(u, v, q, r, s)$  as the coordinate of either  $\phi$  or its matrix  $\Phi$ . On general principles [4, III,8.5] the matrices of  $\phi^{-1}$  in the standard bases for  $\widehat{G}$  and  $\widehat{G} \wedge \widehat{G}$  are  $\Phi^{\text{tr}}$  and  $\Phi^{\text{tr}} \wedge \Phi^{\text{tr}}$ , respectively. For  $\Phi = \Phi(u, v, q, r, s)$  a routine calculation gives

$$(4.3) \quad \Phi^{\text{tr}} = \begin{pmatrix} u & 0 & 0 \\ u^{-1}q & v & 0 \\ s & u^{-1}r & u \end{pmatrix}, \text{ and}$$

$$(4.4) \quad \Phi^{\text{tr}} \wedge \Phi^{\text{tr}} = \begin{pmatrix} uv & 0 & 0 \\ r & u^2 & 0 \\ z & q & uv \end{pmatrix},$$

where  $z = \det \begin{pmatrix} u^{-1}q & v \\ s & u^{-1}r \end{pmatrix}$ . Next we identify  $\mathbb{X}(\triangleleft)$  with  $\mathbb{Z}_p^5$  via the assignment  $x = a_1 e^* + a_2 g^* + b_1 e^* \wedge g^* + b_2 e^* \wedge f^* + b_3 g^* \wedge f^* \mapsto v(x) = (a_1, a_2, b_1, b_2, b_3)$ . We use the notation  $e'_i, e''_j, i = 1, 2, j = 1, 2, 3$  for the standard unit vectors in  $\mathbb{Z}_p^2, \mathbb{Z}_p^3$ , respectively. We begin with  $\mathbb{A}(\triangleleft)$ -orbits in  $\widehat{G}^{C_p}$  and  $\widehat{G} \wedge \widehat{G}$ . We define  $Z'_i, Z''_j, 0 \leq i \leq 2, 0 \leq j \leq 3$  by the formula

$$Z'_i = \{(a_1, a_2) | a_i \neq 0 \text{ and } a_k = 0 \text{ for } k > i > 0\},$$

$$Z''_j = \{(b_1, b_2, b_3) | b_j \neq 0 \text{ and } b_k = 0 \text{ for } k > j > 0\},$$

and  $Z'_0 = \{(0, 0)\}, Z''_0 = \{(0, 0, 0)\}$ . Furthermore we split  $Z''_2$  into the union of  $Z''_{2,k}, k = 0, 1$  where  $Z''_{2,k} = \{(b_1, \zeta^k b_2, 0) | b_2 \in \mathbb{Z}_p^{\bullet 2}\}$ . We let  $\kappa$  denote an element of  $\{1, (2, 0), (2, 1), 3\}$ .

**Lemma 4.6.** *The sets  $Z'_i, Z''_\kappa$  are all the orbits of  $\mathbb{A}(\triangleleft)$  in  $\widehat{G}^{C_p}$  and  $\widehat{G} \wedge \widehat{G}$ , respectively.*

PROOF: First note  $\mathbb{Z}_p^2 = \cup Z'_i$  and  $\mathbb{Z}_p^3 = \cup Z''_\kappa$ . The equalities  $e'_i \mathbb{A}(\triangleleft) = Z'_i, i = 1, 2$  are immediate by (4.3). This proves the first claim.

Similarly, using (4.4) one can derive readily the equalities  $e''_\kappa \mathbb{A}(\triangleleft) = Z''_\kappa$  for  $\kappa = 1, 3$ , and  $\zeta^k e''_2 \mathbb{A}(\triangleleft) = Z''_{2,k}, k = 0, 1$ .  $\square$

Let us write  $Z'_i \times Z''_\kappa$  for the set of vectors  $(v_1, v_2)$  with  $v_1 \in Z'_i, v_2 \in Z''_\kappa$ . These sets are  $\mathbb{A}(\triangleleft)$ -stable and some of them are orbits itself. We list those that are in

**Lemma 4.7.** *For all  $(i, \kappa) \neq (1, (2, k)), (2, 3), k = 0, 1$   $Z'_i \times Z''_\kappa$  is an orbit.*

PROOF: The claim is that for generators  $e', e''$  of  $Z'_i, Z''_\kappa$  in the nonexceptional cases,  $(e', e'')$  generates  $Z'_i \times Z''_\kappa$ . We give details for  $Z'_1 \times Z''_3$ , other cases are treated similarly. Combining (4.3) with (4.4) we obtain

$$(1, 0, 0, 0, 1) \cdot \mathbb{A}(\triangleleft) = \{(u, 0, z, q, uv)\}$$

Now for every element  $(a_1, 0, b_1, b_2, b_3) \in Z'_1 \times Z''_3$  the equations  $u = a_1, uv = b_3, uvr = b_1, q = b_2$ , are obviously solvable. A solution to the equation  $z = b_1$  is provided by  $r = 0$  and  $s = -v^{-1}b_1$ .  $\square$

We pick up  $p - 1$  additional orbits in

**Lemma 4.8.** *Each set  $Z'_1 \times Z''_{2,k}, k = 0, 1$  is a union of  $(p - 1)/2$  orbits.*

PROOF: Say  $k = 0$ . By definition  $Z'_1 \times Z''_{2,0} = \{(a_1, 0; b_1, b_2, 0) | a_1 \in \mathbb{Z}_p^\bullet, b_2 \in \mathbb{Z}_p^{\bullet 2}, b_1 \text{ arbitrary}\}$ , hence  $|Z'_1 \times Z''_{2,0}| = \frac{(p-1)}{2}(p - 1)p$ . For every  $m \in \mathbb{Z}_p^{\bullet 2}$  we let  $z_m = (1, 0; 0, m, 0)$ . By (4.3) and (4.4) for  $\phi = \phi(u, v, q, r, s)$  we have  $z_m \cdot \phi^{-1} = (u, 0, mr, mu^2, 0)$ . A direct count gives  $|z_m \cdot \mathbb{A}(\triangleleft)| = (p - 1)p$ , and one can verify directly that  $z_m \cdot \mathbb{A}(\triangleleft) \cap z_n \cdot \mathbb{A}(\triangleleft) = \emptyset$  for  $m \neq n$ . Since there are  $\frac{p-1}{2}$  orbits of this size, this case is done. For  $i = 1$  one should take  $z'_m = (1, 0; 0, \zeta m, 0)$ .  $\square$

We summarize

**Lemma 4.9.** *There are  $2p + 8$  nontrivial orbits of  $\mathbb{A}(\triangleleft)$  in  $\mathbb{X}(\triangleleft)$ .*

PROOF: The previous two lemmas give  $p + 8$  nontrivial orbits. The rest will come from splitting of the remaining set  $Z'_2 \times Z''_3$ . The latter is defined as  $\{(a_1, a_2, b_1, b_2, b_3) | a_2, b_3 \in \mathbb{Z}_p^\bullet, a_1, b_1, b_2 \text{ arbitrary}\}$ . For every  $k \in \mathbb{Z}_p$  we define  $w_k = (k, 1, 0, 0, 1)$ . Again by (4.3) and (4.4) we have

$$(4.5) \quad w_k \cdot \phi^{-1} = (uk - u^{-1}q, v, z, q, uv).$$

where  $(u, v, q, r, s)$  are the parameters of  $\phi$ . This formula shows that  $w_k \cdot \phi^{-1}$  does not depend on  $r$ . Setting  $r = 0$  we have  $z = -sv$ . It follows easily that  $w_k \cdot \phi^{-1}$  is uniquely determined by  $(u, v, q, s)$ , hence  $|w_k \cdot \mathbb{A}(\triangleleft)| = (p - 1)^2 p^2$ . Furthermore, we claim that  $w_k \cdot \mathbb{A}(\triangleleft) \cap w_l \cdot \mathbb{A}(\triangleleft) = \emptyset$  for  $k \neq l$ . For, suppose

$$(uk - u^{-1}q, v, -sv, q, uv) = (u'l - u'^{-1}q', v', -s'v', q', u'v')$$

for some  $(u, v, q, s)$  and  $(u', v', q', s')$ . Then  $v = v', q = q'$  give  $u = u'$ , hence  $uk = ul$  and therefore  $k = l$ , a contradiction. We conclude that  $|\cup_{0 \leq k \leq p-1} w_k \cdot \mathbb{A}(\triangleleft)| = p^3(p - 1)^2$ . As this is the number of elements in  $Z'_2 \times Z''_3$ , the proof is complete.  $\square$

(4) Orbits of  $\mathcal{G}(\triangleleft)$ . We need to know the action of  $\omega_k = \lambda_k \alpha_k^{-1}$  where  $\lambda_k$  are defined in part (2). Set  $l = k^{-1} \pmod{p}$ .

**Lemma 4.10.** *Action of  $\omega_k$  is described by*

$$\begin{aligned} e^*.\omega_k &= le^*, g^*.\omega_k = lg^* \\ e^* \wedge g^*.\omega_k &= le^* \wedge g^* \\ e^* \wedge f^*.\omega_k &= l^2 e^* \wedge f^* \\ g^* \wedge f^*.\omega_k &= -\binom{l}{2} e^* \wedge g^* + l^2 g^* \wedge f^* \end{aligned}$$

PROOF: By (3.11) for  $x \in \mathbb{X}(\triangleleft)$ ,  $x.\omega_k = (\phi_l \bullet x).\lambda_k$ . For  $x = e^*, g^*, e^* \wedge g^*, e^* \wedge f^*, \phi_l \bullet x = lx$  as these elements are fixed by  $C_p$ . Because  $(t-1)^2 \bullet \widehat{G} \wedge \widehat{G} = 0$  we expand  $\phi_l$  in powers of  $t-1$ , namely  $\phi_l = l + \binom{l}{2}(t-1) + \text{higher terms}$ . One can check  $(t-1) \bullet g^* \wedge f^* = -e^* \wedge g^*$  which gives

$$\phi_l \bullet g^* \wedge f^* = lg^* \wedge f^* - \binom{l}{2} e^* \wedge g^*,$$

By definition of  $\lambda_k$  its matrix is  $\Lambda_k = \text{diag}(1, 1, k)$  (that is the diagonal matrix with entries  $1, 1, k$ ). It follows (see part (3)) that the matrix of  $\lambda_k$  in the standard basis of  $\widehat{G}$  is  $(\Lambda_k^{-1})^{\text{tr}} = \text{diag}(1, 1, l)$ . Applying  $\lambda_k$  to  $\phi_l \bullet x$  as  $x$  runs over the standard bases of  $\widehat{G}$  and  $\mathbb{X}(\triangleleft)$  we complete the proof of the Lemma.  $\square$

The next Proposition completes the proof of Theorem 4.4.

**Proposition 4.11.** *The sets of  $\mathcal{G}(\triangleleft)$  and  $\mathbb{A}(\triangleleft)$ -orbits coincide.*

PROOF: By Corollary 3.13 for every  $x \in \mathbb{X}(\triangleleft)$ ,  $x\mathcal{G}(\triangleleft)$  is a union of orbits  $x.\omega_k \mathbb{A}(\triangleleft)$  for  $1 \leq k \leq p-1$ . Thus it suffices to show  $x.\omega_k \in x\mathbb{A}(\triangleleft)$  for every  $k$  and generators  $x$  of every orbit of  $\mathbb{A}(\triangleleft)$ . We give a sample calculation for  $x = w_m$  of Lemma 4.9. By Lemma 4.10

$$w_m.\omega_k = (lm, l, -\binom{l}{2}, 0, l^2).$$

Now take  $\phi$  with coordinates  $u = l, v = l, q = 0, r = 0, s = l^{-1}\binom{l}{2}$ . Then by (4.5)  $w_m.\phi^{-1} = w_m.\omega_k$  as needed.  $\square$

We move on to the next case

(II)  $G \simeq R_3$ . We denote by  $\triangleleft_r$  the right multiplication in  $R_3$ . This case is sensitive to the prime  $p$ . Let us agree to write  $\mathbb{X}_p$  for  $\mathbb{X}(\triangleleft_r)$  if  $G$  is a  $p$ -group. For  $r \in \mathbb{Z}_p C_p$  we denote by  $\bar{r}$  the image of  $r$  in  $R_3$ . The elements  $e = \bar{1}, f = \overline{(t-1)}, g = \overline{(t-1)^2}$  form a basis for  $R_3$  in which action of  $t$  is defined by  $T = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ . Let  $\{e^*, f^*, g^*\}$  be the dual

basis for  $\widehat{G}$ , and  $\{e^* \wedge f^*, e^* \wedge g^*, f^* \wedge g^*\}$  the induced basis for  $\widehat{G} \wedge \widehat{G}$ . We call all these bases standard. We aim to prove

**Theorem 4.12.** *For  $p > 3$   $\text{Ext}_{[\triangleleft_r]}(\mathbb{k}^{C_p^3}, \mathbb{k}C_p)$  contains  $p + 9$  isoclasses,  $p + 7$  of which are nontrivial, and three nontrivial isoclasses if  $p = 3$ .*

PROOF: Proof will be carried out in steps following the procedure for computing the number of isoclasses.

(1) Classifying groups  $\mathbb{X}_p$ .

**Lemma 4.13.** *If  $p = 3$ , then*

$$\mathbb{X}_3 = \langle e^* \wedge f^*, e^* \wedge g^* \rangle$$

For every  $p > 3$

$$\mathbb{X}_p = \mathbb{Z}_p e^* \oplus \widehat{G} \wedge \widehat{G}$$

PROOF: The matrices of  $t$  in the standard bases of  $\widehat{G}$  and  $\widehat{G} \wedge \widehat{G}$  are  $T^{\text{tr}}$  and  $T^{\text{tr}} \wedge T^{\text{tr}}$ , respectively, with  $T^{\text{tr}} \wedge T^{\text{tr}} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$ . From

this one computes directly  $(t - 1)^3 \bullet \widehat{G} = (t - 1)^3 \bullet \widehat{G} \wedge \widehat{G} = 0$ . Since  $\phi_p(t) = (t - 1)^{p-1}$ , it follows that  $N(G) = 0$  and  $(\widehat{G} \wedge \widehat{G})_N = \widehat{G} \wedge \widehat{G}$  for any  $p > 3$ . Furthermore  $\widehat{G}^{C_p} = \mathbb{Z}_p e^*$  for every  $p$ . Thus as  $\mathbb{X}_p = \widehat{G}^{C_p} / N(\widehat{G}) \oplus (\widehat{G} \wedge \widehat{G})_N$  the second statement of the Lemma follows.

Say  $p = 3$ . Then  $N(\widehat{G}) = (t - 1)^2 \bullet \widehat{G} = \mathbb{Z}_p e^*$ , hence  $\widehat{G}^{C_p} / N(\widehat{G}) = 0$ . Another verification gives  $(\widehat{G} \wedge \widehat{G})_N = \langle e^* \wedge f^*, e^* \wedge g^* \rangle$ .  $\square$

(2) Groups  $\mathbb{A}(\triangleleft_r)$  and  $C(\triangleleft_r)$ . For any ring  $R$  with unity viewed as a right regular  $R$ -module and any right  $R$ -module  $M$  the mapping  $\lambda_M : M \rightarrow \text{Hom}_R(R, M)$  defined by  $x \cdot \lambda_M(m) = mx, x \in R$  is an  $R$ -isomorphism. Setting  $M = R = R_3$  we have  $\mathbb{A}(\triangleleft_r) = \{\lambda_{R_3}(m) | m \in R_3\}$ . Expand  $m$  in the standard basis of  $R_3$ ,  $m = ue + qf + rg$ . Then the

matrix of  $\phi = \lambda_{R_3}(m)$  is  $\Phi = \begin{pmatrix} u & q & r \\ 0 & u & q \\ 0 & 0 & u \end{pmatrix}$ . The matrices of mappings

induced by  $\phi^{-1}$  in  $\widehat{G}$  and  $\widehat{G} \wedge \widehat{G}$  are  $\Phi^{\text{tr}}$  and  $\Phi^{\text{tr}} \wedge \Phi^{\text{tr}}$ . Explicitly

$$(4.6) \quad \Phi^{\text{tr}} = \begin{pmatrix} u & 0 & 0 \\ q & u & 0 \\ r & q & u \end{pmatrix} \text{ and } \Phi^{\text{tr}} \wedge \Phi^{\text{tr}} = \begin{pmatrix} u^2 & 0 & 0 \\ uq & u^2 & 0 \\ q^2 - ur & uq & u^2 \end{pmatrix}$$

We will show that  $C(\triangleleft_r) = \mathbb{Z}_p^\bullet$  by constructing a family of isomorphisms  $\lambda_k : (G, \triangleleft_r) \rightarrow (G, \triangleleft_r^k)$  for every  $k \in \mathbb{Z}_p^\bullet$ . To this end, let us

take  $M = (R_3, \triangleleft_r^k)$  and set  $\lambda_k = \lambda_M(e)$ . By definition of  $\lambda_k$  we have

$$e.\lambda_k = e, f.\lambda_k = e(t^k - 1), g.\lambda_k = e(t^k - 1)^2$$

Using the expansion  $t^k - 1 = k(t - 1) + \binom{k}{2}(t - 1)^2 \pmod{(t - 1)^3}$  we

conclude that  $\Lambda_k = \begin{pmatrix} 1 & 0 & 0 \\ 0 & k & \binom{k}{2} \\ 0 & 0 & k^2 \end{pmatrix}$  is the matrix of  $\lambda_k$  in the standard

basis. We shall need an explicit form of the associated matrices describing the action of  $\lambda_k$  in  $\widehat{G}$  and  $\widehat{G} \wedge \widehat{G}$ , respectively. Put  $l = k^{-1} \pmod{p}$  as usual. Then an easy calculation gives

$$(4.7) \quad (\Lambda_k^{-1})^{\text{tr}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & l & 0 \\ 0 & \binom{l}{2} & l^2 \end{pmatrix},$$

$$(4.8) \quad (\Lambda_k^{-1})^{\text{tr}} \wedge (\Lambda_k^{-1})^{\text{tr}} = \begin{pmatrix} l & 0 & 0 \\ \binom{l}{2} & l^2 & 0 \\ 0 & 0 & l^3 \end{pmatrix}.$$

Unless stated otherwise we assume below that  $p > 3$ . The degenerate case  $p = 3$  follows easily from the general one.

(3) Orbits of  $\mathbb{A}(\triangleleft_r)$  in  $\mathbb{X}_p$ . We identify  $\mathbb{X}_p$  with  $\mathbb{Z}_p^4$  via  $x = ae^* + b_1e^* \wedge f^* + b_2e^* \wedge g^* + b_3g^* \wedge f^* \mapsto (a, b_1, b_2, b_3)$ . We begin by listing all orbits in  $\widehat{G}^{C_p}$  and  $\widehat{G} \wedge \widehat{G}$ , respectively:

$$Z'_0 = \{(0)\}, Z'_1 = \{(a) | a \neq 0\}, Z''_0 = \{(0, 0, 0)\},$$

$$Z''_{ij} = \{(*, \dots, *, \zeta^j b_i, 0, \dots, 0) | b_i \in \mathbb{Z}_p^{\bullet 2}\}, i = 1, 2, 3; j = 0, 1$$

where the  $*$  denotes an arbitrary element of  $\mathbb{Z}_p$ . For more complex orbits we need vectors  $v_k(m) = (1, 0, \dots, m, 0, \dots, 0) \in \mathbb{Z}_p^4$  with the  $m$  filling the  $(k + 1)$ th slot,  $k = 1, 2, 3$  and running over  $\mathbb{Z}_p^\bullet$ .

**Lemma 4.14.** *There are  $3p + 5$  orbits of  $\mathbb{A}(\triangleleft_r)$  in  $\mathbb{X}_p$ , namely*

$$Z'_0 \times Z''_0, Z'_1 \times Z''_0, Z'_0 \times Z''_{ij}, \text{ and } v_k(m)\mathbb{A}(\triangleleft_r), k = 1, 2, 3$$

PROOF: The first two sets are clearly orbits. By (4.6) and every  $i, j$   $(0, \dots, \zeta^j, 0, \dots, 0) \cdot \phi = (0, *, \dots, *, \zeta^j u^2, 0, \dots, 0)$  with the  $*$  standing  $_{i+1}$  for an arbitrary element of  $\mathbb{Z}_p$ . This shows  $Z'_0 \times Z''_{ij}$  is the orbit of  $(0, \dots, \zeta^j, 0, \dots, 0) \cdot \phi$ . Applying (4.6) again we have  $_{i+1}$

$$(4.9) \quad v_k(m) \cdot \phi = (u, *, \dots, *, u^2 m, 0, \dots, 0)$$

From this one can see easily that  $v_k(m)\mathbb{A}(\triangleleft_r)$  has  $(p - 1)p^{k-1}$  elements. Another verification gives  $v_k(m)\mathbb{A}(\triangleleft_r) \cap v_k(n)\mathbb{A}(\triangleleft_r) = \emptyset$  for  $m \neq n$ . Let



us define  $Z_i'' = Z_{i0}'' \cup Z_{i1}''$  and observe that  $|Z_i''| = (p-1)p^{i-1}$  which gives  $|Z_1' \times Z_i''| = (p-1)^2 p^{i-1}$ . Evidently  $v_i(m) \in Z_1' \times Z_i''$  for all  $m$  and therefore comparing cardinalities we arrive at the equality  $Z_1' \times Z_i'' = \bigcup_m v_i(m) \mathbb{A}(\triangleleft_r)$ . But clearly  $\mathbb{X}_p = \bigcup_l Z_l' \times Z_i'', l = 0, 1; 0 \leq i \leq 3$  which completes the proof.  $\square$

(4) End of the proof.

**Proposition 4.15.** *The nonzero orbits of  $\mathcal{G}(\triangleleft_r)$  in  $\mathbb{X}_p$  are as follows:*

$$Z_0' \times Z_{ij}'', Z_0' \times Z_2'', Z_1' \times Z_0'', Z_1' \times Z_2'', Z_1' \times Z_{3j}'', \text{ and } v_1(m) \mathbb{A}(\triangleleft_r),$$

where  $i = 1, 3, j = 0, 1$  and  $m$  runs over  $\mathbb{Z}_p^\bullet$ .

PROOF: By Corollary 3.13 we need to determine the  $\mathbb{A}(\triangleleft_r)$ -orbit containing  $v\omega_k$  where  $v$  runs over a set of generators of  $\mathbb{A}(\triangleleft_r)$ -orbits of Lemma 4.14, and  $\omega_k = \lambda_k \alpha_k^{-1}, 2 \leq k \leq p-1$ .

(i) For  $\mathbb{A}(\triangleleft_r)$ -orbits  $Z_1' \times Z_0''$  and  $Z_0' \times Z_{ij}''$  generators are  $e^*$  and  $v_{ij} = (0, 0, \dots, \zeta_{i+1}^j, \dots, 0)$ , respectively. In view of  $e^*$  and  $e^* \wedge f^*$  being fixed points for the action of  $t$ , and by (4.7), (4.8) it is immediate that

$$(4.10) \quad e^* \omega_k = l e^* \text{ and } v_{1j} \omega_k = l^2 v_{1j},$$

hence  $Z_0' \times Z_{1j}''$  and  $Z_1' \times Z_0''$  are  $\mathcal{G}(\triangleleft_r)$ -orbits.

(ii) Next we take the generator  $v_{20} = e^* \wedge g^*$ . Noting that  $(t-1)^2 \bullet e^* \wedge g^* = 0$ , we use the expansion  $\phi_l = l + \binom{l}{2}(t-1) \pmod{(t-1)^2}$  to derive

$$\phi_l \bullet e^* \wedge g^* = c e^* \wedge f^* + l e^* \wedge g^*, \quad c \in \mathbb{Z}_p.$$

Applying  $\lambda_k$  to the last equation we find with the help from (4.8)

$$(4.11) \quad e^* \wedge g^* \omega_k = c' e^* \wedge f^* + l^3 e^* \wedge g^*, \text{ for some } c' \in \mathbb{Z}_p.$$

The last equation shows that  $v_{20} \omega_k \in v_{21} \mathbb{A}(\triangleleft_r)$  if  $l$ , hence  $k$ , is not a square, and  $v_{20} \omega_k \in v_{20} \mathbb{A}(\triangleleft_r)$ , otherwise. This means  $v_{20} \mathcal{G}(\triangleleft_r) = Z_0' \times (Z_{20}'' \cup Z_{21}'') = Z_0' \times Z_2''$  as needed.

The argument for the generator  $v_{3j} = (0, 0, 0, \zeta^j) = \zeta^j f^* \wedge g^*$  of  $Z_0' \times Z_{3j}''$  is almost identical. Using the expansion  $\phi_l = l + c_1(t-1) + c_2(t-1)^2 \pmod{(t-1)^3}$  we derive  $\phi_l \bullet f^* \wedge g^* = (c_1 + c_2) e^* \wedge f^* + c_1 e^* \wedge g^* + l f^* \wedge g^*$ . Applying  $\lambda_k$  we have by (4.8)

$$(4.12) \quad f^* \wedge g^* \omega_k = c_1' e^* \wedge f^* + c_1 l^2 e^* \wedge g^* + l^4 f^* \wedge g^*, \quad c_1', c_1 \in \mathbb{Z}_p.$$

which shows  $\zeta^j f^* \wedge g^* \omega_k \in Z_{3j}'$  for every  $k$ , hence  $Z_0' \times Z_{3j}''$  is a  $\mathcal{G}(\triangleleft_r)$ -orbit.

(iii) We pause to mention that the above arguments settle the  $p = 3$ -case. For, since  $\mathbb{X}_3 = \langle e^* \wedge f^*, e^* \wedge g^* \rangle$ , by parts (i) and (ii) it has three nonzero orbits, namely  $Z_{1j}'', Z_2'', j = 0, 1$ .

(iv) Here we take  $v_1(m) = (1, m, 0, 0)$ . Calculations in part (i) give  $v_1(m).\omega_k = (l, l^2m, 0, 0) \in v_1(m)\mathbb{A}(\triangleleft_r)$  by (4.9). That is,  $v_1(m)\mathbb{A}(\triangleleft_r)$  is a  $\mathcal{G}(\triangleleft_r)$ -orbit for every  $m \in \mathbb{Z}_p^\bullet$ .

It remains to show that the last three sets of the Proposition are  $\mathcal{G}(\triangleleft_r)$ -orbits.

(v)  $Z'_1 \times Z''_2$  is an orbit. By Lemma 4.14  $Z'_1 \times Z''_2 = \bigcup_m v_2(m)\mathbb{A}(\triangleleft_r)$  where  $v_2(m) = e^* + me^* \wedge g^*$ . Note that by (4.10) and (4.11) there holds  $v_2(m).\omega_k = (l, c', l^3m, 0)$ . On the other hand we have by (4.6)  $v_2(n).\phi = (u, uq, u^2n, 0)$  where  $u, q$  run over  $\mathbb{Z}_p^\bullet$  and  $\mathbb{Z}_p$ , respectively. For every  $l$  choosing  $\phi = \phi(l, u^{-1}c', 0)$  and  $n = lm$  we obtain  $v_2(m).\omega_k = v_2(n)\phi^{-1}$ . Letting  $k$  hence  $l$  run over  $\mathbb{Z}_p^\bullet$  we see that  $v_2(m)\mathcal{G}(\triangleleft_r) = \bigcup_n v_2(n)\mathbb{A}(\triangleleft_r)$  which completes the proof.

(vi) Here we show that each  $Z'_1 \times Z''_{3j}$  is an orbit. By (4.10) and (4.12)

$$v_3(m).\omega_k = (1, 0, 0, m).\omega_k = (l, c', c'', ml^4) \text{ for some } c', c'' \in \mathbb{Z}_p.$$

We seek an  $n$  such that

$$(4.13) \quad v_3(m).\omega_k = v_3(n).\phi \text{ for some } \phi \in \mathbb{A}(\triangleleft_r).$$

By (4.6)  $v_3(n).\phi = (u, q^2 - ur, uq, u^2n)$  where  $u, q, r$  take arbitrary values in  $\mathbb{Z}_p^\bullet$  and  $\mathbb{Z}_p$ , respectively. Choosing  $u, q, r$  such that  $u = l, q^2 - ur = c', uq = c''$  and  $n = ml^2$  fullfils (4.13). This yields the equality (\*)  $v_3(m)\mathcal{G}(\triangleleft_r) = \bigcup_{n \in m\mathbb{Z}_p^{\bullet 2}} (1, 0, 0, n)\mathbb{A}(\triangleleft_r)$ . Therefore depending

on  $m \in \mathbb{Z}_p^{\bullet 2}$ , or  $m \notin \mathbb{Z}_p^{\bullet 2}$  the right hand side of (\*) equals to  $Z'_1 \times Z''_{30}$  or  $Z'_0 \times Z''_{31}$ , respectively.  $\square$

#### 4.2.2. $G = \mathbb{Z}_{p^e} \oplus \mathbb{Z}_p$ .

Our immediate goal is to classify nontrivial Hopf algebras in  $\text{Ext}(\mathbb{k}C_p, \mathbb{k}^{\mathbb{Z}_{p^2} \oplus \mathbb{Z}_p})$ . We find it convenient to enlarge the scope of the problem by taking  $G = \mathbb{Z}_{p^e} \oplus \mathbb{Z}_p$  for *any*  $e \geq 2$  as the amount of effort is the same as for  $e = 2$ . As before our prime is odd, the even case is done in [11]. The end result is-

**Theorem 4.16.** *There are  $2p+8$  distinct Hopf algebras in  $\text{Ext}(\mathbb{k}C_p, \mathbb{k}^G)$  if either  $p > 3$  or  $e \geq 3$ , and 16 if  $p = 3$  and  $e = 2$ .*

PROOF: We break up the proof in steps.

(1) Our first task is to describe the set of classes  $[\triangleleft]$  and their associated groups  $\mathbb{A}(\triangleleft), C(\triangleleft)$ . We need several preliminary observations. Every representation  $\triangleleft : C_p \rightarrow \text{Aut}(G)$  is determined by  $\triangleleft(t)$ . Let us write  $\Gamma_e = \text{Aut}(\mathbb{Z}_{p^e} \oplus \mathbb{Z}_p)$  and  $\Gamma_e(p)$  for the set of all elements of

order  $p$  in  $\Gamma_e$ . It is clear that the mapping  $\triangleleft \mapsto \triangleleft(t)$  sets up a bijection between the set  $\{\triangleleft\}$  and  $\Gamma_e(p)$ , and we will identify both sets. Furthermore the class  $\text{eq}(\triangleleft)$  of representations equivalent to  $\triangleleft$  corresponds to the  $\Gamma_e$ -conjugacy class of  $\triangleleft(t)$  denoted  $\triangleleft(t)^\Gamma$ . It follows that  $[\triangleleft] = \bigcup_{1 \leq k \leq p-1} \triangleleft(t^k)^\Gamma$ .

$G$  has a natural basis  $e_1, e_2$  comprised of generators of  $\mathbb{Z}_{p^e}, \mathbb{Z}_p$ , respectively. Let  $\epsilon$  be an endomorphism of  $G$ . We use the standard matrix representation of endomorphisms of direct sums to associate to  $\epsilon$  a matrix  $M(\epsilon) = \begin{pmatrix} a & \bar{b} \\ cp^{e-1} & \bar{d} \end{pmatrix}$  relative to the basis  $\{e_1, e_2\}$  with  $a, b, c, d \in \mathbb{Z}_{p^e}$  and the bar over an  $n \in \mathbb{Z}_{p^e}$  denoting the image of  $n$  in  $\mathbb{Z}_p$ . The correspondence  $\epsilon \mapsto M(\epsilon)$  extends to an isomorphism under the multiplication rule

$$\begin{pmatrix} a & \bar{b} \\ cp^{e-1} & \bar{d} \end{pmatrix} \begin{pmatrix} a' & \bar{b}' \\ c'p^{e-1} & \bar{d}' \end{pmatrix} = \begin{pmatrix} aa' + c'bp^{e-1} & \overline{ab' + bd'} \\ (ca' + dc')p^{e-1} & \overline{dd'} \end{pmatrix}$$

**Lemma 4.17.**  $\Gamma_e$  is the set of all matrices  $\begin{pmatrix} a & \bar{b} \\ cp^{e-1} & \bar{d} \end{pmatrix}$  satisfying  $\overline{ad} \neq 0$

PROOF: The natural epimorphism  $G \rightarrow \mathbb{Z}_p \oplus \mathbb{Z}_p$  induces a homomorphism  $\pi : \Gamma_e \rightarrow \text{Aut}(\mathbb{Z}_p^2)$  via  $\begin{pmatrix} a & \bar{b} \\ cp^{e-1} & \bar{d} \end{pmatrix} \mapsto \begin{pmatrix} \bar{a} & \bar{b} \\ 0 & \bar{d} \end{pmatrix}$ . If  $\gamma$  is invertible then so is  $\pi(\gamma)$ , and the latter is equivalent to  $\overline{ad} \neq 0$ . Conversely, if  $\overline{ad} \neq 0$ , then  $a, d$  are units in  $\mathbb{Z}_{p^e}$ . One can check easily a factorization

$$(4.14) \quad \begin{pmatrix} a & \bar{b} \\ cp^{e-1} & \bar{d} \end{pmatrix} = \begin{pmatrix} 1 & \bar{0} \\ a^{-1}cp^{e-1} & \bar{1} \end{pmatrix} \begin{pmatrix} a & \bar{0} \\ 0 & \bar{d} \end{pmatrix} \begin{pmatrix} a & \overline{a^{-1}b} \\ 0 & \bar{d} \end{pmatrix}$$

which completes the proof.  $\square$

**Lemma 4.18.** (i)  $\Gamma_e(p)$  is the set of all matrices  $\begin{pmatrix} 1 + ip^{e-1} & \bar{j} \\ kp^{e-1} & \bar{1} \end{pmatrix}$ ;  
(ii)  $|\Gamma_e(p)| = p^3$  regardless of  $e$ ;  
(iii)  $\Gamma_e(p)$  is a normal subgroup of  $\Gamma_e$ .

PROOF: (i) Assume  $M = \begin{pmatrix} a & \bar{b} \\ cp^{e-1} & \bar{d} \end{pmatrix}$  has order  $p$ . Then  $\pi(M)$  has also order  $p$  which implies  $\bar{a}^p = \bar{1} = \bar{d}^p$ , hence  $\bar{d} = \bar{1}$  and  $a \equiv 1 \pmod{p}$ . A straightforward induction on  $r$  gives

$$(4.15) \quad M^r = \begin{pmatrix} a^r + bc \binom{r}{2} p^{e-1} & \overline{rb} \\ rcp^{e-1} & \bar{1} \end{pmatrix}$$

whence  $M^p = I$  iff  $a^p = 1$ . But this condition on  $a$  is equivalent to  $a = 1 + ip^{e-1}$ . (ii) and (iii) are easy consequences of (i).  $\square$

By the above Lemma  $\Gamma_e(p)$  does not depend on  $e$ . We will omit  $e$  from its notation below.

**Remark 4.19.** All parts of this Lemma fail for  $p = 2$ .

**Proposition 4.20.** *The set  $\{\lhd\}$  consists of five nontrivial elements.*

PROOF: (1) The first class of action is the one generated by  $\lhd_1$  with  $\lhd_1(t) = \text{diag}(1 + p^{e-1}, 1)$ , the diagonal matrix with entries  $1 + p^{e-1}, \bar{1}$  on the main diagonal in that order. Using (4.14) one can see easily that the matrices  $\text{diag}(1 + kp^{e-1}, \bar{1})$  form the center of  $\Gamma(p)$ . Since  $\lhd_1(t^k) = \text{diag}(1 + kp^{e-1}, \bar{1})$  it follows that  $[\lhd_1] = \{\lhd_1^k | 1 \leq k \leq p-1\}$ . As  $\lhd_1(t)$  is in the center  $\mathbb{A}(\lhd_1) = \Gamma_e, C(\lhd_1) = \{1\}$  hence  $\mathcal{G}(\lhd_1) = \mathbb{A}(\lhd_1)$ .

(2) Let  $T_\ell$  be the subset of lower triangular matrices in  $\Gamma(p)$ ,  $Z$  the center of  $\Gamma(p)$  and  $T'_\ell = T_\ell \setminus Z$ . Fix one action  $\lhd_\ell$  defined by  $\lhd_\ell(t) = \begin{pmatrix} 1 & \bar{0} \\ p^{e-1} & \bar{1} \end{pmatrix}$ .

**Lemma 4.21.** (i)  $T'_\ell = \lhd_\ell^\Gamma$ ;

(ii)  $I(\lhd_\ell, \lhd_\ell^k) \neq \emptyset$  for every  $k$ . In particular,  $\text{diag}(1, \overline{k^{-1}}) \in I(\lhd_\ell, \lhd_\ell^k)$ ;

(iii)  $\mathbb{A}(\lhd_\ell) = \left\{ \begin{pmatrix} a & \bar{0} \\ cp^{e-1} & \bar{a} \end{pmatrix} \right\}$  and  $C(\lhd_\ell) = A_p$ .

PROOF: (i) Pick another action  $\lhd$  with  $\lhd(t) = \begin{pmatrix} 1 + ip^{e-1} & \bar{0} \\ jp^{e-1} & \bar{1} \end{pmatrix}, j \neq 0$ .

Matrices  $\begin{pmatrix} 1 & \bar{0} \\ kp^{e-1} & \bar{1} \end{pmatrix}$  lie in the center of  $T_\ell$ . By (4.14)  $\lhd_\ell^\Gamma$  equals to  $\{\lhd_\ell^\gamma\}$  where  $\gamma$  runs over all upper triangular matrices in  $\Gamma_e$ . Choose a  $\gamma = \begin{pmatrix} a & \bar{b} \\ 0 & \bar{d} \end{pmatrix}$  and observe that  $\gamma \in I(\lhd_\ell, \lhd)$  iff (\*)  $\lhd_\ell(t)\gamma = \gamma\lhd(t)$ . One can see by a direct calculation that (\*) holds iff

$$\begin{aligned} ai + bj &\equiv 0 \pmod{p} \\ a &\equiv jd \pmod{p}. \end{aligned}$$

These congruences are equivalent to the conditions  $b \equiv -aij^{-1} \pmod{p}$ ,  $d \equiv aj^{-1} \pmod{p}$  which gives (\*\*)  $I(\lhd_\ell, \lhd) = \left\{ \begin{pmatrix} a & -\overline{aij^{-1}} \\ cp^{e-1} & \overline{aj^{-1}} \end{pmatrix} \right\}$ .

(ii) Take  $\lhd = \lhd_\ell^k$  and observe that  $i = 0, j = k$  for this action. Specifying  $a = 1, c = 0$  in (\*\*) yields (2).

(iii) Set  $\lhd = \lhd_\ell$  and note that  $i = 0, j = 1$  in this case. Then (\*\*) gives the assertion.  $\square$

(3) It remains to describe conjugacy classes in  $\Gamma(p) \setminus T_\ell$ . Elements of this set are distinguished by the property-

**Lemma 4.22.**  $\triangleleft(t) \in \Gamma(p) \setminus T_\ell$  iff the  $C_p$ -module  $(G, \triangleleft)$  is cyclic.

PROOF: In one direction take  $\triangleleft(t) = \begin{pmatrix} 1 + ip^{e-1} & \bar{j} \\ kp^{e-1} & \bar{1} \end{pmatrix} \in \Gamma(p) \setminus T_\ell$ . Then  $\bar{j} \neq 0$  and therefore from  $e_1 \triangleleft t = (1 + ip^{e-1})e_1 + je_2$  we have  $e_2 = j^{-1}e_1 \triangleleft (t - (1 + ip^{e-1}))$  showing that  $G$  is generated by  $e_1$ .

Conversely, assume  $\bar{j} = 0$ . The subgroup  $\langle pe_1 \rangle$  is a  $C_p$ -submodule of  $G$ . Further,  $G/\langle pe_1 \rangle$  is a trivial  $C_p$ -module isomorphic to  $\mathbb{Z}_p \oplus \mathbb{Z}_p$  which proves  $(G, \triangleleft)$  is not cyclic.  $\square$

We associate to an action  $\triangleleft \in \Gamma(p) \setminus T_\ell$  with  $\triangleleft(t) = \begin{pmatrix} 1 + ip^{e-1} & \bar{j} \\ kp^{e-1} & \bar{1} \end{pmatrix}$  the element  $m(\triangleleft) = jk$  of  $\mathbb{Z}_{p^e}$ . For an  $n \in \mathbb{Z}_{p^e}$  we define  $I(n)$  to be the ideal of  $R$  generated by  $p(t-1)$ ,  $(t-1)^2 - np^{e-1}$  and  $(t-1)^3$ .  $\overline{m}(\triangleleft)$  is an invariant of  $\triangleleft(t)^\Gamma$  according to

**Lemma 4.23.** (i) In the foregoing notation  $(G, \triangleleft) \simeq R/I(m)$ .

(ii) Two actions  $\triangleleft, \triangleleft'$  in  $\Gamma(p) \setminus T_\ell$  are equivalent iff  $\overline{m}(\triangleleft) = \overline{m}(\triangleleft')$ .

PROOF: Let  $R = \mathbb{Z}_{p^e}C_p$ . Since  $G = e_1R$  by the preceeding Lemma, both the assertions follow from the equality  $I(m) = \text{ann}_{Re_1}$  for  $m = m(\triangleleft)$ . In one direction, a simple calculation gives that  $pe_1$  is a fixed point and  $e_1 \triangleleft (t-1)^2 = jkp^{e-1}e_1$ . It follows that  $e_1 \triangleleft g(t) = 0$  for every generator  $g(t)$  of  $I(m)$  from the above list, whence  $I(m) \subset \text{ann}_{Re_1}$ . In the opposite direction we note every element of  $R$  is congruent to some  $n + m(t-1)$ ,  $n, m \in \mathbb{Z}_{p^e}$  modulo  $I(m)$ . Were  $\text{ann}_{Re_1} \neq I(m)$ , there would be an  $n + m(t-1)$  with  $e_1 \triangleleft (n + m(t-1)) = 0$ , yet  $n \neq 0$  or  $m \not\equiv 0 \pmod{p}$ . But  $e_1 \triangleleft (n + m(t-1)) = (n + mip^{e-1})e_1 + mje_2 = 0$  holds iff  $m \equiv 0 \pmod{p}$  and  $n = 0$  proving the equality in question.  $\square$

We single out three actions in  $\Gamma(p) \setminus T_\ell$ ,

$$(4.16) \quad \triangleleft^0 = \begin{pmatrix} 1 & \bar{1} \\ p^{e-1} & \bar{1} \end{pmatrix}, \triangleleft^1 = \begin{pmatrix} 1 & \bar{1} \\ p^{e-1} & \bar{1} \end{pmatrix}, \triangleleft^\zeta = \begin{pmatrix} 1 & \zeta \\ p^{e-1} & \bar{1} \end{pmatrix}.$$

The next lemma completes the proof of the Proposition

**Lemma 4.24.**  $\Gamma(p) \setminus T_\ell$  is the union of  $[\triangleleft^0]$ ,  $[\triangleleft^1]$  and  $[\triangleleft^\zeta]$ .

PROOF: By the formula (4.15) we have  $m(\triangleleft^r) = r^2m(\triangleleft)$ . The preceeding Lemma makes it clear that sets  $[\triangleleft^q]$ ,  $q = 0, 1, \zeta$  correspond to the orbits of  $\mathbb{Z}_p^{\bullet 2}$  in  $\mathbb{Z}_p$ , namely  $\{0\}, \mathbb{Z}_p^{\bullet 2}, \zeta\mathbb{Z}_p^{\bullet 2}$ .  $\square$

(4) We complete the proof of the main theorem of this section by computing the classifying groups and orbits for each of the five classes of actions. To begin with we select a basis for  $\widehat{G}$  dual to  $\{e_i\}$  denoted by  $\{e_i^*\}$ .  $C_p$  and  $\Gamma_e$  act in  $\widehat{G}$  by (1.4) and  $(f.\gamma)(g) = f(g\gamma^{-1})$ ,  $f \in \widehat{G}$ ,  $g \in G$ , respectively. These actions extend to  $\text{Alt}(G) = \widehat{G} \wedge \widehat{G}$  in the usual way. We note that  $\text{Alt}(G)$  is generated by  $\beta = e_1^* \wedge e_2^*$  and the latter form has order  $p$ . For the future references we record

**Lemma 4.25.** (i) Let  $\begin{pmatrix} a & \bar{b} \\ cp^{e-1} & \bar{d} \end{pmatrix}$  be the matrix of either  $\gamma \in \Gamma$  or  $t$  relative to  $\{e_i\}$ . The matrix of  $\gamma^{-1}$  or  $t$  relative to  $\{e_i^*\}$  is  $\begin{pmatrix} a & \bar{c} \\ bp^{e-1} & \bar{d} \end{pmatrix}$   
(ii) There holds  $\beta.\gamma^{-1} = ad\beta$ ,  $t.\beta = \beta$ , and  $\text{Alt}_N(G) = \text{Alt}(G)$ .

PROOF: (i) is seen by a simple calculation. For (ii) we use part (i) to calculate  $e_1^* \wedge e_2^*.\gamma^{-1} = (ae_1^* + ce_2^*) \wedge (bp^{e-1}e_1^* + de_2^*) = ade_1^* \wedge e_2^*$ . Similarly  $t.e_1^* \wedge e_2^* = ade_1^* \wedge e_2^*$ . However in the case of  $t$ ,  $a = 1 + ip^{e-1}$  and  $d = 1$  by Lemma 4.18, which gives the second formula. Therefore  $\phi_p(t).\beta = p\beta = 0$  which proves the last assertion.  $\square$

(i) We take up the action  $\triangleleft_1$  of Proposition 4.20(1).

**Lemma 4.26.**  $\text{Ext}_{[\triangleleft_1]}(\mathbb{K}C_p, \mathbb{K}^G)$  contains two distinct nontrivial Hopf algebras.

PROOF: A simple calculation gives  $\widehat{G}^{C_p} = \langle pe_1^*, e_2^* \rangle$ . As for  $N(\widehat{G})$  we have  $\phi_p(t).e_2^* = pe_2^* = 0$  and  $\phi_p(t).e_1^* = (\sum_{i=0}^{p-1} (1 + p^{e-1})^i)e_1^* = pe_1^*$ . It follows that  $\widehat{G}^{C_p}/N(\widehat{G}) = \langle \bar{e}_2^* \rangle$  where  $\bar{e}_2^* = e_2^* + N(\widehat{G})$ . As noted in Proposition 4.20(1)  $\mathcal{G}(\triangleleft_1) = \mathbb{A}(\triangleleft_1) = \Gamma_e$ . By Lemma 4.25  $\bar{e}_2^*.\gamma^{-1} = d\bar{e}_2^*$  and  $\beta.\gamma^{-1} = ad\beta$ . We conclude that  $\mathbb{X}(\triangleleft_1) \simeq \mathbb{Z}_p \oplus \mathbb{Z}_p$  with the action  $(c_1, c_2).\gamma = (dc_1, adc_2)$ . Now it is immediate that there are two nontrivial (i.e.  $c_2 \neq 0$ ) orbits, viz.  $\{(0, c_2)\}$  and  $\{c_1, c_2 | c_1c_2 \neq 0\}$ .  $\square$

(ii) Next we consider  $\triangleleft_\ell$  from Proposition 4.20(2).

**Lemma 4.27.** There are  $p + 1$  distinct nontrivial Hopf algebras in  $\text{Ext}_{[\triangleleft_\ell]}(\mathbb{K}C_p, \mathbb{K}^G)$ .

PROOF: One can see easily with the help from Lemma 4.25  $\widehat{G}^{C_p} = \langle pe_1^*, e_2^* \rangle$ . Further  $N(e_2^*) = pe_2^* = 0$  and  $N(e_1^*) = pe_1^*$ . All in all we have  $\widehat{G}^{C_p}/N(\widehat{G}) = \langle \bar{e}_2^* \rangle$  and  $\mathbb{X}(\triangleleft_\ell) = \langle \bar{e}_2^*, \beta \rangle$ . Using definition (3.11) we have  $\bar{e}_2^*.\omega_k = (\phi_{k^{-1}}(t).\bar{e}_2^*).\lambda_k$  where  $\lambda_k = \text{diag}(1, \mathbb{K}^{-1})$  by Lemma 4.21. Since  $\bar{e}_2^*$  is a fixed point,  $\phi_{k^{-1}}(t).\bar{e}_2^* = k^{-1}\bar{e}_2^*$  and by Lemma 4.25  $\bar{e}_2^*.\lambda_k = k\bar{e}_2^*$ , hence  $\bar{e}_2^*$  is fixed by  $\omega_k$ . A similar calculation gives  $\beta.\omega_k = \beta$ . Thus  $\mathcal{G}(\triangleleft_\ell)$ -orbits coincide with  $\mathbb{A}(\triangleleft_\ell)$ -orbits. For the latter

we take  $\phi \in \mathbb{A}(\triangleleft_\ell)$  as in Lemma 4.21(iii) and apply Lemma 4.25 to get  $\overline{e_2^*} \cdot \phi^{-1} = \overline{a} \overline{e_2^*}$  and  $\beta \cdot \phi^{-1} = \overline{a}^2 \beta$ . It transpires that  $\mathbb{X}(\triangleleft_\ell) \simeq \mathbb{Z}_p^2$  with the action on the right by  $(c_1, c_2) \cdot \phi^{-1} = (\overline{a}c_1, \overline{a}^2c_2)$ . Now the argument in Proposition 4.1 completes the proof.  $\square$

(iii) Finally we tackle actions (4.16). We determine the groups  $\mathbb{A}(\triangleleft^q), C(\triangleleft^q), q = 0, 1, \zeta$  and sets of intertwiners  $\{\lambda_k | k \in C(\triangleleft^q)\}$ .

**Lemma 4.28.** (i)  $\mathbb{A}(\triangleleft^q) = \left\{ \begin{pmatrix} a & \overline{b} \\ bqpe^{-1} & \overline{a} \end{pmatrix} \right\};$

(ii)  $C(\triangleleft^0) = A_p$  and for every  $1 \leq k \leq p-1$   $I(\triangleleft^0, (\triangleleft^0)^k) \ni \begin{pmatrix} 1 & \overline{0} \\ 0 & k \end{pmatrix};$

(iii) If  $q \neq 0$ , then  $C(\triangleleft^q) = \{1, p-1\}$  and  $I(\triangleleft^q, (\triangleleft^q)^{p-1}) \ni \begin{pmatrix} 1 & \overline{0} \\ qp^{e-1} & -\overline{1} \end{pmatrix}$

PROOF: (i)  $\mathbb{A}(\triangleleft^q)$  is the group of units of  $\text{End}_R(R/I(q))$ . We pointed out in Theorem 4.12(2) that  $\text{End}_R(R/I(q))$  consists of mappings  $\lambda(u) : x \mapsto ux, u, x \in R/I(q)$ . By Lemma 4.23(i)  $u = a\overline{1} + b(\overline{t} - 1)$  where  $\overline{r} = r + I(q)$  for  $r \in R$ . It is immediate that the matrix of  $\lambda(u)$  relative to  $\{\overline{1}, \overline{t} - 1\}$  is the one in part (i).

(ii) and (iii) By Lemma 4.23  $C(\triangleleft^q) = \{k | k^2q = q\}$ . Clearly this formula implies  $C(\triangleleft^0) = A_p$  and  $C(\triangleleft^q) = \{1, p-1\}$  for  $q \neq 0$ . Let us write  $\overline{R} = R/I(q)$  and denote by  $\overline{R}^{(k)}$  the  $C_p$ -module  $(\overline{R}, (\triangleleft^q)^k)$ . By general principles for every  $k \in C(\triangleleft^q)$ ,  $\text{Hom}_R(\overline{R}, \overline{R}^{(k)})$  consists of mappings  $\lambda(u), u \in \overline{R}$ . Pick  $\lambda(\overline{1})$  and observe that for every suitable  $k$  the matrices of  $\lambda(\overline{1})$  in the basis  $\{\overline{1}, \overline{t} - 1\}$  are as given in (ii) and (iii), respectively.  $\square$

The last step of the proof of Theorems 4.16 and 4.3 is-

**Lemma 4.29.** (i) *There are  $p+1$  nontrivial distinct Hopf algebras in  $\text{Ext}_{[\triangleleft^0]}(\mathbb{k}C_p, \mathbb{k}^G)$ ;*

(ii) *There are two nontrivial distinct Hopf algebras in  $\text{Ext}_{[\triangleleft^q]}(\mathbb{k}C_p, \mathbb{k}^G)$  for  $q = 1, \zeta$  if either  $p > 3$  or  $e \geq 3$ , and four otherwise.*

PROOF: (i) One can see easily that  $\widehat{G}^{C_p}(\triangleleft^0) = \langle e_1^* \rangle$  and  $N(\widehat{G}(\triangleleft^0)) = pe_1^*$ , hence  $\widehat{G}^{C_p}(\triangleleft^0)/N(\widehat{G}(\triangleleft^0)) = \langle \overline{e_1^*} \rangle$ . By Lemma 4.25(ii)  $\mathbb{X}(\triangleleft^0) = \langle \overline{e_1^*}, \beta \rangle$ . Pick a  $\gamma \in \mathbb{A}(\triangleleft^0)$  as in Lemma 4.28. By Lemma 4.25 there holds  $\overline{e_1^*} \cdot \gamma^{-1} = \overline{a} \overline{e_1^*}$  and  $\beta \cdot \gamma^{-1} = \overline{a}^2 \beta$ . This type of action occurred in Proposition 4.1 whose argument yields  $p+1$  nontrivial  $\mathbb{A}(\triangleleft^0)$ -orbits. Turning to  $\mathcal{G}(\triangleleft^0)$ -orbits, pick a  $\lambda_k = \text{diag}(1, k)$  from the preceding lemma. Since  $\overline{e_1^*}, \beta$  are fixed by  $t$  we have  $\overline{e_1^*} \cdot \omega_k = (\phi_{k^{-1}} \cdot \overline{e_1^*}) \cdot \lambda_k = k^{-1} \overline{e_1^*}$  and  $\beta \cdot \omega_k = (\phi_{k^{-1}} \cdot \beta) \cdot \lambda_k = k^{-2} \beta$ . This shows that  $\mathcal{G}(\triangleleft^0)$ -orbits coincide with  $\mathbb{A}(\triangleleft^0)$  ones, and the proof is complete.

(ii) A straightforward calculation gives  $\widehat{G}^{C_p}(\triangleleft^q) = \langle pe_1^* \rangle$ . For calculation of  $N(\widehat{G}(\triangleleft^q))$  we employ (4.15) which gives readily that

$$\phi_p(t).e_1^* = \left[ \sum_{r=0}^{p-1} (1 + q \binom{r}{2} p^{e-1}) \right] e_1^* + \left( \sum_{r=0}^{p-1} r \right) e_2^*$$

As  $\sum_{r=0}^{p-1} r = \binom{p}{2}$  and  $pe_2^* = 0$  we conclude

$\phi_p(t).e_1^* = (p + q(\sum_{r=0}^{p-1} \binom{r}{2})p^{e-1})e_1^*$ . Similarly one can derive

$$\phi_p(t).e_2^* = q \left( \sum_{r=0}^{p-1} r \right) p^{e-1} e_1^* + pe_2^* = 0$$

Next we note that an elementary calculation gives  $\sum_{r=0}^{p-1} \binom{r}{2} = \binom{p}{3}$ . Let us put  $c(p) = p + q \binom{p}{3} p^{e-1}$ . We observe that if  $p > 3$ , then  $c(p) \equiv p \pmod{p^e}$ . For  $p = 3$  and either  $e \geq 3$  or  $e = 2$  and  $q = 1$ ,  $c(3) = 3u$ , where  $u$  is a unit in  $\mathbb{Z}_{p^e}$ . In the exceptional case  $e = 2$  and  $q = 2$ ,  $c(3) = 9$ . This translates into  $\phi_p(t).e_1^* = pue_1^*$  for all  $p, e, q$ , except for the exceptional case where  $\phi_3(t).e_1^* = 0$ . We conclude that  $N(\widehat{G}(\triangleleft^q)) = \langle pe_1^* \rangle$  in the regular case and it is zero, otherwise. In consequence

$$\mathbb{X}(\triangleleft^1) = \langle \beta \rangle \text{ for all } p, e$$

$$\mathbb{X}(\triangleleft^\zeta) = \langle \beta \rangle \text{ if } p > 3 \text{ or } e \geq 3$$

$$\mathbb{X}(\triangleleft^2) = \langle 3e_1^*, \beta \rangle \text{ if } p = 2 = e.$$

By Lemmas 4.25(ii), 4.28(i)  $\beta.\phi^{-1} = \bar{a}^2\beta$  for every  $\phi \in \mathbb{A}(\triangleleft^q)$ . It follows that there are two nontrivial  $\mathbb{A}(\triangleleft^q)$ -orbits in  $\mathbb{X}(\triangleleft^q)$  in the regular case and also for  $\mathbb{X}(\triangleleft^1)$  in all cases, namely  $\{cq\beta | c \in \mathbb{Z}_p^{\bullet 2} \text{ for } q = 1, \zeta\}$ . Using Lemma 4.28(iii) it is immediate that  $\beta.\omega_{p-1} = \beta$ . That says  $\mathcal{G}(\triangleleft^q)$ -orbits coincide with  $\mathbb{A}(\triangleleft^q)$ -orbits. In the exceptional case  $3e_1^*.\phi^{-1} = \bar{a}(3e_1^*)$  and  $3e_1^*.\omega_2 = -3e_1^*$ . It follows that  $\mathbb{A}(\triangleleft^2)$  and  $\mathcal{G}(\triangleleft^2)$  act on  $\mathbb{X}(\triangleleft^2)$  by  $(c_1, c_2).\phi^{-1} = (\bar{a}c_1, \bar{a}^2c_2)$  and  $(c_1, c_2).\omega_2 = (-c_1, c_2)$  with the usual identification  $\mathbb{X}(\triangleleft^2) \simeq \mathbb{Z}_3^2$ . By the argument of Proposition 4.1 there are four nontrivial  $\mathbb{A}(\triangleleft^2)$ -orbits. One can check directly that the mapping  $(c_1, c_2) \mapsto (-c_1, c_2)$  preserves the orbits, completing the proof.  $\square$

## 5. SOME OLD CLASSIFICATION RESULTS REVISITED

The first result concerns the G. Kac's 8-dimensional Hopf algebra [8, 19] which we denote by  $H_8$ .

**Theorem 5.1.** *There is a unique semisimple, nontrivial 8-dimensional Hopf algebra.*



PROOF: It is easy to see that every Hopf algebra  $H$  as in the Theorem is isomorphic to  $\mathbb{k}^4 \oplus M_2(\mathbb{k})$  as algebra where  $M_2(\mathbb{k})$  is the algebra of  $2 \times 2$  matrices. Applying this remark to  $H^*$  we conclude that  $H^*$  has exactly 4 characters, hence  $G(H)$  has order 4. Thus  $H$  is almost abelian, hence  $H \in \text{Ext}(\mathbb{k}C_2, \mathbb{k}^{G(H)})$ . By Theorem 3.12(II) the number of nontrivial isotypes in  $\text{Ext}_{[\triangleleft]}(\mathbb{k}C_2, \mathbb{k}^G)$  equals to the number of nontrivial  $\mathbb{A}(\triangleleft)$ -orbits in  $H_c^2(\triangleleft)$  for every action  $\triangleleft$  of  $C_2$  on  $G$ . By Corollary 2.4 that number coincides with the number of nontrivial  $\mathbb{A}(\triangleleft)$ -orbits in  $\mathbb{X}(\triangleleft)$ . For every cyclic group  $C_n$ ,  $\text{Alt}(C_n)$  is trivial. Hence, were  $G = C_4$  we would have  $\mathbb{X}(\triangleleft) = \widehat{G}^{C_2}/N(\widehat{G})$  by Lemma 3.16(ii) and therefore  $\mathbb{X}(\triangleleft)$  does not have nontrivial orbits. We take up the remaining case  $G = G(H) = C_2 \times C_2$ . Let  $\{x_1, x_2\}$  be a basis for  $G$  and  $\{x_1^*, x_2^*\}$  its dual. There is only one equivalence class of actions on  $G$ . We choose the action  $x_1 \triangleleft t = x_2, x_2 \triangleleft t = x_1$ . A routine verification gives  $\widehat{G}^{C_2} = N(\widehat{G}) = \langle x_1^* x_2^* \rangle$ . Thus by Lemma 3.16  $\mathbb{X}(\triangleleft) \simeq \underline{a}(Z_N^2(\triangleleft))$  and by Proposition 2.5(3) we have  $\underline{a}(Z_N^2(\triangleleft)) = \text{Alt}_N(G)$ . Further, it is immediate that  $\text{Alt}_N(G) = \text{Alt}(G)$  and the latter consists of one nonzero element. This shows that  $\mathbb{X}(\triangleleft)$  has one nontrivial  $\mathbb{A}(\triangleleft)$ -orbit, and the proof is complete.  $\square$

With a small additional effort one can give a presentation of  $H_8$  by generators and relations. For two vectors  $a = x_1^{j_1} x_2^{j_2}, b = x_1^{k_1} x_2^{k_2}$  we let  $\det(a, b) = j_1 k_2 - j_2 k_1$ .

**Proposition 5.2.**  *$H_8$  is generated as algebra by  $x_1^*, x_2^*, t$  subject to the relations*

$$\begin{aligned} x_1^{*2} &= x_2^{*2} = t^2 = 1 \\ tx_1^* t^{-1} &= x_2^*, tx_2^* t^{-1} = x_1^* \end{aligned}$$

*The coalgebra structure is specified by*

$$\Delta(t) = \left( \sum_{a,b \in G} \iota^{-\det(a,b)} p_a \otimes p_b \right) t \otimes t, \text{ where } \iota^2 = -1.$$

*In addition the equations  $S(x_i^*) = x_i^*, i = 1, 2, S(t) = t$  and  $\epsilon(x_1^*) = \epsilon(x_2^*) = \epsilon(t) = 1$  determine the antipode and augmentation.*

PROOF: Since  $H_8$  is a special cocentral extensions  $H_8 = \widehat{\mathbb{k}G} \# \mathbb{k}C_2$  as algebra. With  $t$  a generator of  $C_2$  the algebra relations follow immediately. By (1.8)

$$\Delta(t) = \left( \sum_{a,b \in G} \tau(t, a, b) p_a \otimes p_b \right) t \otimes t \text{ where } \tau(t, a, b) \in \mathbb{X}(\triangleleft). \text{ As } \mathbb{X}(\triangleleft) \text{ has}$$

only one nonzero element, the latter provided by Proposition 2.5(3ii), we have  $\tau(t, a, b) = s_{1,2} \delta g$ . A straightforward calculation gives

$$\tau(t, a, b) = \iota^{-\det(a, b)}.$$

We find the antipode by using [23, Prop. 4.7]. In our case, i.e. for a special cocentral extension, the formula specializes to  $S(p_at) = \tau^{-1}(t, a^{-1}, a)p_{a^{-1}\triangleleft}t^{-1}$ . Since  $a^2 = 1$  and  $\tau(t, a, a) = 1$ , we obtain  $S(t) = \sum_a S(p_at) = \sum_a p_{a\triangleleft}t = t$ . The rest of the Proposition is self-evident.  $\square$

A. Masuoka [19] presents  $H_8$  by a different set of generators and relations. The two are related by replacing  $t$  with  $z = gx_1^*t$ . The set  $\{x_1^*, x_2^*, z\}$  generates  $H_8$  and one can derive all relations of [19, Thm. 2.13], with one exception, viz.  $S(z) = \frac{1}{2}(-\epsilon + x_1^* + x_2^* + x_1^*x_2^*)z$ . We leave the details to the reader.

We take up the problem of classifying isotypes of Hopf algebras  $H$  of dimension  $2n^2$  with  $G(H) = \mathbb{Z}_n \times \mathbb{Z}_n$  for an odd  $n$ . Put differently we want to determine the isotypes of  $\text{Ext}(\mathbb{k}C_2, \mathbb{k}^{\mathbb{Z}_n \times \mathbb{Z}_n})$ . We let  $G = \mathbb{Z}_n \times \mathbb{Z}_n$ .

Following the general procedure we split up the argument into steps.

(1) A survey of actions.

We will assume  $n = p_1^{e_1} \cdots p_m^{e_m}$  is the prime decomposition of  $n$ . We let  $G(i)$  denote the  $p_i$ -primary summand of  $G$ . Clearly  $G(i) = \mathbb{Z}_{p_i^{e_i}} \oplus \mathbb{Z}_{p_i^{e_i}}$  and  $G = \oplus G(i)$ . Every  $G(i)$  is invariant under any automorphism of  $G$ , in particular under any action of  $C_2$ . Since every  $p_i$  is odd  $\mathbb{Z}_{p_i^{e_i}}C_2 = \mathbb{Z}_{p_i^{e_i}}\epsilon_0 \oplus \mathbb{Z}_{p_i^{e_i}}\epsilon_{-1}$  where  $\epsilon_0 = \frac{1+t}{2}$ ,  $\epsilon_{-1} = \frac{1-t}{2}$ . Idempotents  $\epsilon_\nu$  induce a splitting  $G(i) = G(i)\epsilon_0 \oplus G(i)\epsilon_{-1}$  into a direct sum of subgroups on which  $t$  acts as  $\pm \text{id}$ . Therefore for every action  $\triangleleft$  we can write  $G$  as

$$(5.1) \quad G = G_0 \oplus G_{-1} \oplus G_{0,-1}, \text{ where}$$

$$\begin{aligned} G_0 &= \oplus \{G(i) \mid t|_{G(i)} = \text{id}\}, \quad G_{-1} = \oplus \{G(i) \mid t|_{G(i)} = -\text{id}\}, \text{ and} \\ G_{0,-1} &= \oplus \{G(i) \mid t|_{G(i)} \neq \pm \text{id}\}. \end{aligned}$$

Every equivalence class of actions is determined by its decomposition (5.1).

(2) Classifying groups.

First we show that  $\widehat{G}^{C_2}/N(\widehat{G}) = (0)$ . Pick  $\chi \widehat{G}^{C_2}$ . Then  $N(\chi) := (1+t).\chi = 2\chi$ . Since 2 is a unit in  $\mathbb{Z}_n$ ,  $\chi \in N(\mathcal{G})$ , which proves our assertion. By Lemma 3.16(iii)  $\mathbb{X}(\triangleleft) = \text{Alt}_N(G)$ . Consider an alternate mapping  $\beta : G \times G \rightarrow \mathbb{Z}_n$ . It is apparent that  $\beta(g, h) = 0$  whenever  $g, h$  lie in different components  $G(i)$  of decomposition (5.1). For  $g, h \in G_0$   $(1+t).\beta(g, h) = 2\beta(g, h)$  and similarly for if  $g, h \in G_{-1}$ . It transpires that  $(1+t).\beta(g, h) = 0$  iff  $\beta(g, h) = 0$  for every  $\beta : G_\nu \times G_\nu \rightarrow \mathbb{Z}_n$ ,  $\nu = 0, -1$ . We conclude that  $\mathbb{X}(\triangleleft) = 0$  if  $G_{0,-1} = 0$ .

The above discussion shows that  $\text{Alt}_N(G) = \text{Alt}_N(G_{0,-1})$ . Let us renumber the prime divisors of  $n$  so that  $G_{0,-1} = \bigoplus_{i=1}^r G(i)$ . We noted above that  $G(i) = G(i)\epsilon_0 \oplus G(i)\epsilon_{-1}$  and since  $\mathbb{Z}_{p_i^{e_i}}$  is an indecomposable group,  $G(i)\epsilon_\nu \simeq \mathbb{Z}_{p_i^{e_i}}$ . Therefore we can select a basis  $\{a_i, b_i\}$  of  $G(i)$  with  $a_i, b_i$  generating  $G(i)\epsilon_0, G(i)\epsilon_{-1}$ , respectively and both of order  $p_i^{e_i}$ . Set  $a = \sum a_i, b = \sum b_i$  and observe that  $a, b$  generate subgroups  $G_{0,-1}\epsilon_\nu, \nu = 0, -1$ , respectively. Let us write  $n(\triangleleft) = \prod \{p_i^{e_i} | t|_{G(i)} \neq \pm \text{id}\}$ . Set  $a = \sum a_i, b = \sum b_i$  and observe that  $a, b$  generate subgroups  $G_{0,-1}\epsilon_\nu, \nu = 0, -1$ , respectively. In addition both subgroups  $\langle a \rangle, \langle b \rangle$  are cyclic of order  $n(\triangleleft)$ , hence  $G_{0,-1} \simeq \mathbb{Z}_{n(\triangleleft)} \times \mathbb{Z}_{n(\triangleleft)}$ . It follows that  $\text{Alt}(G_{0,-1})$  is cyclic on a generator, say,  $\beta_0$  defined by  $\beta_0(a, b) = 1_{\mathbb{Z}_{n(\triangleleft)}}$ . The calculation  $(1+t).\beta_0(a, b) = \beta_0(a, b) + \beta(a, -b) = 0$  gives the equality  $\text{Alt}_N(G_{0,-1}) = \text{Alt}(G_{0,-1})$ . It follows that  $\mathbb{X}(\triangleleft) = \text{Alt}(G_{0,-1}) \simeq \mathbb{Z}_{n(\triangleleft)}$ . We observe that since  $\mathbb{X}(\triangleleft) \simeq H_c^2(\mathbb{k}C_2, \mathbb{k}^G, \triangleleft)$  that formula implies a result of A. Masuoka [22, Thm. 2.1] on  $\text{Opext}(\mathbb{k}C_2, \mathbb{k}^G)$ .

We summarize

**Theorem 5.3.** (1) *If  $\triangleleft$  is such that  $G_{0,-1} = 0$ , then  $\text{Ext}_{[\triangleleft]}(\mathbb{k}C_2, \mathbb{k}^G)$  has a unique Hopf algebra  $\mathbb{k}[G \rtimes C_2]$  where  $G \rtimes C_2$  is the semidirect product with respect to  $\triangleleft$ .*

(2) *For  $\triangleleft$  with a nonzero  $G_{0,-1}$  the isotypes in  $\text{Ext}_{[\triangleleft]}(\mathbb{k}C_2, \mathbb{k}^G)$  correspond bijectively to the subgroups of  $\mathbb{Z}_{n(\triangleleft)}$ . The trivial subgroup of  $\mathbb{Z}_{n(\triangleleft)}$  corresponds to a unique trivial Hopf algebra  $\mathbb{k}[G \rtimes C_2]$ .*

PROOF: It remains to compute the orbits of  $\mathbb{A}(\triangleleft)$  in  $\text{Alt}(G_{0,-1})$ . First off, every  $\phi \in \mathbb{A}(\triangleleft)$  preserves  $G_{0,-1}\epsilon_\nu$ , whence

$$a\phi = ua, \quad b\phi = vb \text{ for some } u, v \in \mathbb{Z}_{n(\triangleleft)}^\bullet.$$

Therefore  $(\beta.\phi)(a, b) := \beta(a\phi^{-1}, b\phi^{-1}) = u^{-1}v^{-1}\beta(a, b)$ . This shows that transvering action of  $\mathbb{A}(\triangleleft)$  along the isomorphism  $\beta \mapsto \beta(a, b) : \text{Alt}(G_{0,-1}) \xrightarrow{\sim} \mathbb{Z}_{n(\triangleleft)}$  we get the action  $m.\phi = u^{-1}v^{-1}m, m \in \mathbb{Z}_{n(\triangleleft)}$ . It becomes clear that orbits are exactly sets of generators of cyclic subgroups of  $\mathbb{Z}_{n(\triangleleft)}$ , which completes the proof.  $\square$

## 6. APPENDICES

### Appendix 1: Crossed product splitting of abelian extensions

**Proposition 6.1.** *Let  $H$  be an extension of  $\mathbb{k}F$  by  $\mathbb{k}^G$ . Then  $H$  is a crossed product of  $\mathbb{k}F$  over  $\mathbb{k}^G$ .*

PROOF: First observe that  $H$  is a Hopf-Galois extension of  $\mathbb{k}^G$  by  $\mathbb{k}F$  via  $\rho_\pi = (\text{id} \otimes \pi)\Delta_H : H \rightarrow H \otimes \mathbb{k}F$ , see e.g. the proof of [24,

3.4.3], hence by [24, 8.1.7]  $H$  is a strongly  $F$ -graded algebra. Setting  $H_x = \{h \in H \mid \rho_\pi(h) = h \otimes x\}$  we have  $H = \bigoplus_{x \in F} H_x$  with  $H_1 = \mathbb{k}^G$  and  $H_x H_{x^{-1}} = \mathbb{k}^G$  for all  $x \in F$ . Next for every  $a \in G$  we construct elements  $u(a) \in H_x$ ,  $v(a) \in H_{x^{-1}}$  such that

$$\begin{aligned} u(a)v(a) &= p_a, p_a u(a) = u(a), v(a)p_a = v(a), \text{ and} \\ u(a)v(b) &= 0 \text{ for all } a \neq b. \end{aligned}$$

Indeed, were all  $uv, u \in H_x, v \in H_{x^{-1}}$  lie in  $\text{span}\{p_b \mid b \neq a\}$ , then so would  $H_x H_{x^{-1}}$ , a contradiction. Therefore for every  $a \in G$  there are  $u \in H_x, v \in H_{x^{-1}}$  such that  $uv = \sum c_b p_b, c_a \neq 0$ . Setting  $u(a) = \frac{1}{c_a} p_a u, v(a) = v p_a$  we get elements satisfying the first three properties stated above. Furthermore, the last property also holds because  $u(a)v(b) = p_a u(a)v(b)p_b = p_a p_b u(a)v(b) = 0$ . It follows that the elements  $u_x = \sum_{a \in G} u(a), v_x = \sum_{a \in G} v(a)$  satisfy  $u_x v_x = 1$  hence, as  $H$  is finite-dimensional,  $v_x u_x = 1$  as well. Thus  $u_x$  is a 2-sided unit in  $H_x$ .

Now define  $\gamma : \mathbb{k}F \rightarrow H$  by  $\gamma(x) = \frac{1}{\epsilon_H(u_x)} u_x$ . One can see immediately that  $\gamma$  is a convolution invertible mapping satisfying  $\rho_\pi \circ \gamma = \gamma \otimes \text{id}, \gamma(1_F) = 1$  and  $\epsilon_H \circ \gamma = \epsilon_F$ . Thus  $\gamma$  is a section of  $\mathbb{k}F$  in  $H$ , which completes the proof.  $\square$

## Appendix 2: Non-splitting of $\mathbb{X}(\triangleleft)$ as $\mathbb{A}(\triangleleft)$ -module for $p = 2$

We take a closer look at the exact sequence  $\widehat{G}^{C_p}/N(\widehat{G}) \rightarrow \mathbb{X}(\triangleleft) \rightarrow \underline{a}(Z_N^2(\triangleleft))$  of Lemma 3.16. We know by Theorem 2.5 that for  $p > 2$   $\underline{a}(Z_N^2(\triangleleft)) = \text{Alt}_N(G)$  and the above sequence splits up, that is  $\mathbb{X}(\triangleleft) \simeq \widehat{G}^{C_p}/N(\widehat{G}) \times \text{Alt}_N(G)$  as  $\mathbb{A}(\triangleleft)$ -modules. We want to show that this is not the case for  $p = 2$ .

Let  $G$  be an elementary 2-group of rank  $n$  and  $\triangleleft$  be the trivial action. By the argument of part (2) of Proposition 2.5 our assumptions imply  $\widehat{G}^{C_p}/N(\widehat{G}) = \widehat{G}$  and  $\underline{a}(Z_N^2(\triangleleft)) = \text{Alt}(G)$ . The main result of this Appendix is

**Theorem 6.2.** *Let  $G$  be a 2-elementary group of rank  $n > 2$ . The sequence of  $\mathbb{A}(\text{triv})$ -modules*

$$\widehat{G} \rightarrow \mathbb{X}(\text{triv}) \rightarrow \text{Alt}(G)$$

*does not split.*

PROOF: Will be given in steps. To simplify notation we write  $\mathbb{X}$  and  $\mathbb{A}$  for  $\mathbb{X}(\text{triv})$  and  $\mathbb{A}(\text{triv})$ .

(1) Let  $S$  be a copy of  $\text{Alt}(G)$  in  $Z^2(G, \mathbb{k}^\bullet)$  constructed in Proposition 2.5(2). Clearly  $S \subset Z_N^2(\text{triv})$  and complements  $B_N^2(\text{triv})$ . Passing on

to  $\mathbb{X}$  the image of  $S$ , denoted by  $S$ , forms a complement to  $\widehat{G}$ . Fix a basis  $\{x_i | 1 \leq i \leq n\}$  of  $G$  and let  $\{x_i^* | 1 \leq i \leq n\}$  be its dual in  $\widehat{G}$ . Observe that  $\Phi : B_N^2(\text{triv}) \rightarrow \widehat{G}$  acts in the present case by  $\Phi(\delta f) = f^2$ . Let  $b_i : G \times G \rightarrow \mathbb{k}^\bullet$  be the bimultiplicative map defined by

$$b_i(x_i, x_i) = -1, b_i(x_k, x_l) = 1 \text{ for } (k, l) \neq (i, i).$$

**Lemma 6.3.** (1)  $\Phi(b_i) = x_i^*$  for all  $i$ ;  
 (2)  $\text{Alt}(G) \subset \ker \Phi$ .

PROOF: (1) Recall  $B^2(G, \mathbb{k}^\bullet)$  is the subgroup of all symmetric functions of  $Z^2(G, \mathbb{k}^\bullet)$ , hence  $b_i \in B^2(G, \mathbb{k}^\bullet)$  and therefore  $b_i = \delta f_i$  for some  $f_i : G \rightarrow \mathbb{k}^\bullet$ . Then

$$b_i(x_j, x_j) = \delta f_i(x_j, x_j) = f_i(x_j) f_i(x_j) f_i(x_j^2)^{-1} = f_i^2(x_j).$$

We note that as  $b_i^2 = \epsilon$ ,  $b_i$  lies in  $B_N^2(G, \mathbb{k}^\bullet)$ , hence  $f_i^2 \in \widehat{G}$  and as  $f_i^2(x_j) = (-1)^{\delta_{ij}} f_i^2 = x_i^*$ . This proves (1).

(2) Elements of  $\text{Alt}(G)$  are symmetric functions, hence  $\text{Alt}(G) \subset B^2(G, \mathbb{k}^\bullet)$ . By part (1) for every  $\alpha = \delta f \in \text{Alt}(G)$   $\Phi(\alpha) = f^2 = \epsilon$  as  $\alpha(x, x) = 1$ .  $\square$

(2) Let  $\widehat{G} \wedge \widehat{G}$  be the exterior square of  $\widehat{G}$ . There is a well-known identification  $\text{Alt}(G) = \widehat{G} \wedge \widehat{G}$ . In the additive notation  $\widehat{G} \wedge \widehat{G}$  has a standard basis  $x_i^* \wedge x_j^*$  where  $x_i^* \wedge x_j^*(x_k, x_l) = \delta_{ik} \delta_{jl}$ . Passing on to  $S$  we write  $s_{x_i^* \wedge x_j^*}$  as  $s_{\langle i, j \rangle}$  which by the definition of  $s_\alpha$  is given by

$$s_{\langle i, j \rangle}(x_k, x_l) = \begin{cases} 1, & \text{if } \{k, l\} = \{i, j\} \text{ and } k < l \\ 0, & \text{else.} \end{cases}$$

We note the equality  $s_{\langle i, j \rangle} = s_{\langle j, i \rangle}$ . Pick  $\phi \in \mathbb{A}$  and let  $\phi^* : \widehat{G} \rightarrow \widehat{G}$  be the transpose of  $\phi$ , i.e.  $(\chi \cdot \phi^*)(g) = \chi(g \cdot \phi)$ ,  $\chi \in \widehat{G}, g \in G$ . If  $M(\phi)$  is the matrix of  $\phi$  in the basis  $\{x_k\}$  then  $M(\phi^*) = M(\phi)^{\text{tr}}$  is the matrix of  $\phi^*$  in the dual basis. Therefore the matrix of the mapping  $\widehat{\phi}$ ,  $(\chi \cdot \widehat{\phi})(g) = \chi(g \cdot \phi^{-1})$  induced by  $\phi$  in  $\widehat{G}$  is  $M(\phi^{-1})^{\text{tr}}$ . Next we describe action of  $\mathbb{A}$  in  $\mathbb{X}$

**Lemma 6.4.** Suppose  $\phi \in \mathbb{A}$  and  $M(\phi^{-1}) = (a_{kl})$ .  $\phi$  acts in  $\mathbb{X}$  as follows

$$(6.1) \quad s_{\langle i, j \rangle} \cdot \phi = s_{x_i^* \wedge x_j^*} \cdot \phi + \sum_{k=1}^n a_{ki} a_{kj} x_k^*.$$

PROOF: One can see easily that the mapping  $\underline{a}$  is  $\mathbb{A}$ -linear therefore  $\underline{a}(s_{\langle i, j \rangle} \cdot \phi) = x_i^* \wedge x_j^* \cdot \phi$ . We also know  $\underline{a}(s_\alpha) = \alpha$  for every  $\alpha \in \text{Alt}(G)$

which gives

$$(6.2) \quad s_{\langle i, j \rangle} \cdot \phi = s_{x_i^* \wedge x_j^*} \cdot \phi + \bar{b},$$

where  $\bar{b} := b \ker \Phi \in B_N^2(\text{triv}) / \ker \Phi$ . By Lemma 6.3 the set  $\{\bar{b}_k\}$  forms a basis for  $B_N^2(\text{triv}) / \ker \Phi$ , hence  $\bar{b} = \sum_{k=1}^n c_k \bar{b}_k$ ,  $c_k \in \mathbb{Z}_2$ . Since  $s_\alpha(x_k, x_k) = 0$  for every  $\alpha$  and  $k$ , evaluating (6.2) at  $(x_k, x_k)$  yields

$$\begin{aligned} c_k &= s_{\langle i, j \rangle} \cdot \phi(x_k, x_k) = s_{\langle i, j \rangle}(x_k \phi^{-1}, x_k \phi^{-1}) \\ &= s_{\langle i, j \rangle} \left( \sum_i a_{ki} x_i, \sum_j a_{kj} x_j \right) = a_{ki} a_{kj} \end{aligned}$$

A reference to Lemma 6.3(1) completes the proof.  $\square$

It is well known that  $\mathbb{A}$  is generated by transvections, linear mappings  $t_{pq} : x_p \rightarrow x_p + x_q, x_r \rightarrow x_r, r \neq p$ . Since  $t_{pq}^{-1} = t_{pq}$  and the matrix of  $t_{pq}^*$  is  $M(t_{pq})^{\text{tr}}$  we have readily

$$\begin{aligned} x_k^* \cdot t_{pq} &= x_k, k \neq q, \\ x_q^* \cdot t_{pq} &= x_q^* + x_p^*. \end{aligned}$$

We see that  $t_{pq}$  induces the transvection  $t_{qp}$  in  $\widehat{G}$ . In consequence we have

**Lemma 6.5.** *Action of transvections on the standard basis of  $\text{Alt}(G)$  is given by*

$$\begin{aligned} x_i^* \wedge x_j^* \cdot t_{pq} &= x_i^* \wedge x_j^* \text{ if } q \neq i, j \text{ or } (p, q) = (i, j), (j, i) \\ x_i^* \wedge x_j^* \cdot t_{pi} &= x_i^* \wedge x_j^* + x_p^* \wedge x_j^*, p \neq j \\ x_i^* \wedge x_j^* \cdot t_{pj} &= x_i^* \wedge x_j^* + x_i^* \wedge x_p^*, p \neq i. \quad \square \end{aligned}$$

With the help of Lemma 6.4 we deduce

**Lemma 6.6.** *Action of transvections on generators of  $S$  is given by*

$$\begin{aligned} s_{\langle i, j \rangle} \cdot t_{pq} &= s_{\langle i, j \rangle}, \text{ if } q \neq i, j \\ s_{\langle i, j \rangle} \cdot t_{ij} &= s_{\langle i, j \rangle} + x_i^* \\ s_{\langle i, j \rangle} \cdot t_{ji} &= s_{\langle i, j \rangle} + x_j^* \\ s_{\langle i, j \rangle} \cdot t_{pi} &= s_{\langle i, j \rangle} + s_{\langle p, j \rangle} \\ s_{\langle i, j \rangle} \cdot t_{pj} &= s_{\langle i, j \rangle} + s_{\langle i, p \rangle}. \end{aligned}$$

PROOF: In view of Lemmas 6.4 and 6.5 we need only to calculate the  $\widehat{G}$ -components. If  $(p, q) \neq (i, j), (j, i)$ , then for the entries of  $M(t_{pq})$  there holds  $a_{ki} = 0$  or  $a_{kj} = 0$  for every  $k$ . In  $M(t_{ij}), M(t_{ji})$  we have  $a_{ki} a_{kj} = 1$  only for  $k = i, j$ , respectively.  $\square$

(3) End of the Proof. Suppose there is an  $\mathbb{A}$ -linear section  $\zeta : \text{Alt}(G) \rightarrow \mathbb{X}$  splitting  $\underline{a}$ . Say

$$(6.3) \quad \zeta(x_i^* \wedge x_j^*) = \chi_{ij} + s_{\langle i,j \rangle}, \chi_{ij} \in \widehat{G}.$$

Then there holds

$$(6.4) \quad \zeta(x_i^* \wedge x_j^* \cdot t_{pq}) = (\chi_{ij} + s_{\langle i,j \rangle}) \cdot t_{pq} \text{ for all } p, q.$$

Let us expand  $\chi_{ij}$  in the basis  $\{x_k^*\}$ ,

$$\chi_{ij} = \sum_k c_k^{ij} x_k^*.$$

Observe the equality  $\chi_{ij} \cdot t_{pq} = \chi_{ij} + c_q^{ij} x_p^*$ . Next specialize (6.4) to  $p = i, q = j$  or  $p = j, q = i$ . Then Lemmas 6.5 and 6.6 give  $c_j^{ij} x_i^* + x_i^* = 0$  and  $c_i^{ij} x_j^* + x_j^* = 0$ , respectively. We see that  $c_i^{ij} = c_j^{ij} = 1$ , that is  $\chi_{ij} = x_i^* + x_j^* + \sum_{k \neq i,j} c_k^{ij} x_k^*$ . Note that if  $n = 2$  we have shown that

$\mathbb{Z}_2(x_1^* + x_2^* + s_{\langle 1,2 \rangle})$  is an  $\mathbb{A}$ -complement to  $\widehat{G}$ . Suppose  $n > 2$ . For every  $q \neq i, j$  we have by (6.4) and Lemmas 6.5 and 6.6 the equality

$$\chi_{ij} + s_{\langle i,j \rangle} = \chi_{ij} \cdot t_{iq} + s_{\langle i,j \rangle} \cdot t_{iq}$$

Using  $\chi_{ij} \cdot t_{iq} = \chi_{ij} + c_q^{ij} x_i^*$  and  $s_{\langle i,j \rangle} \cdot t_{iq} = s_{\langle i,j \rangle}$  we conclude  $c_q^{ij} = 0$ . Thus  $\chi_{ij} = x_i^* + x_j^*$  for all  $i, j$ .

Next pick  $p \neq i, j$ , and apply (6.4). We have

$$\zeta(x_i^* \wedge x_j^* + x_p^* \wedge x_j^*) = (x_i^* + x_j^* + s_{\langle i,j \rangle}) \cdot t_{pi}$$

which in turn gives the equality

$$x_i^* + x_j^* + s_{\langle i,j \rangle} + x_p^* + x_j^* + s_{\langle p,j \rangle} = x_i^* + x_p^* + x_j^* + s_{\langle i,j \rangle} + s_{\langle p,j \rangle},$$

hence  $x_j^* = 0$ , a contradiction.

On the evidence we have so far we propose

**Conjecture.** Suppose  $G = \prod_{i=1}^m C_{p^{e_i}}^{n_i}$ ,  $e_1 < \dots < e_m$ . Let  $N(G, p)$  be

the number of almost abelian Hopf algebras of dimension  $|G|p$ . The function  $N(G, p)$  is a polynomial over  $\mathbb{Z}$  of degree  $\leq e_m$  for all  $p \geq e_1 + \dots + e_m$ .

## REFERENCES

- [1] N. Andruskiewitsch, Notes on extensions of Hopf algebras, *Can. J. Math.* **48**(1)(1996), 3-42.
- [2] F. R. Beyl and J. Tappe, Group Extensions, Representations, and the Schur Multiplier, *Lecture Notes in Mathematics* **958**, Springer-Verlag, 1982.
- [3] R.J. Blattner, M. Cohen and S. Montgomery, Crossed Product and Inner Actions of Hopf Algebras, *Trans. Amer. Math. Soc* **298**(2)(1986), 671-711.

- [4] N. Bourbaki, Elements of Mathematics, Algebra I, Springer-Verlag, 1989.
- [5] N.P. Byott, Cleft extensions of Hopf algebras, *J. Algebra* **157**(1993), 405-429.
- [6] M. Hall, Jr., "The Theory of Groups", The Macmillan Company, New York, 1959.
- [7] I. Hofstetter, Extensions of Hopf algebras and their cohomological description, *J. Algebra* **164**(1994), 264-298.
- [8] G.I. Kac and V.G. Paljutkin, Finite ring groups, *Trans. Moscow Math. Soc.* **15**(1966), 251-294.
- [9] G.I. Kac, Certain arithmetic properties of ring groups, *Functional Anal. Appl.* **6** (1972), 158-160.
- [10] Y. Kashina, Classification of semisimple Hopf algebras of dimension 16, *J. Algebra* **232**(2000), 617-663.
- [11] Y. Kashina, On semisimple Hopf Algebras of Dimension  $2^m$ , *Algebras and Representation Theory* **6**(2003), 393-425.
- [12] Y. Kashina, G. Mason and S. Montgomery, Computing the Frobenius-Schur indicator for abelian extensions of Hopf algebras, *J. Algebra* **251**(2002), 888-913.
- [13] T. Kobayashi and A. Masuoka, A result extended from groups to Hopf algebras, *Tsukuba J. Math* **21** (1997), 55-58.
- [14] R.G. Larson and D.E. Radford, Semisimple cosemisimple Hopf algebras, *Amer. J. Math.* **110**(1988), 187-195.
- [15] S. MacLane, "Homology", Die Grundlehren der Mathematischen Wissenschaften **114**, Springer-Verlag, 1963.
- [16] M. Mastnak, Hopf algebra extensions arising from semi-direct products of groups, *J. Algebra* **251**(2002), 413-434.
- [17] A. Masuoka and Y. Doi, Generalization of cleft comodule algebras, *Comm. Algebra* **20**(1992), 3703-3721.
- [18] A. Masuoka, Self-dual Hopf algebras of dimension  $p^3$  obtained by extensions, *J. Algebra* **178**(1995), 791-806.
- [19] A. Masuoka, Semisimple Hopf algebras of dimension 6,8, *Israel J. Math.*, **92** (1995), 361-373.
- [20] A. Masuoka, The  $p^n$  theorem for semisimple Hopf algebras, *Proc. Amer. Math. Soc.*, **124**(3)(1996), 735-737.
- [21] A. Masuoka, Some further classification results on semisimple Hopf algebras, *Comm. Algebra* **24**(1)(1996), 307-329.
- [22] A. Masuoka, Calculations of some groups of Hopf algebra extensions, *J. Algebra* **178**(1997), 568-588.
- [23] A. Masuoka, Extensions of Hopf algebras (Lecture Notes, University of Cordoba, 1997) Notas Mat.No. 41/99, FaMAF Uni. Nacional de Cordoba, 1999.
- [24] S. Montgomery, Hopf Algebras and their Actions on Rings, in: *CMBS Reg. Conf. Ser. Math.* **82**, AMS, 1993.
- [25] C. Nastasescu and F. Van Oystaeyen, On strongly graded rings and crossed products, *Comm. Algebra* **10** (1982), 2085-2106.
- [26] W.D. Nichols and M.B. Zoeller, A Hopf algebra freeness theorem, *Amer. J. Math* **111**(1989), 381-385.
- [27] H.-J. Schneider, Some remarks on exact sequences of quantum groups, *Comm. Algebra* (9)**21**(1993), 3337-3358.



- [28] H.-J. Schneider, A normal basis and transitivity of crossed products for Hopf algebras, *J. Algebra* **152**(1992), 289-312.
- [29] D. Stefan, The set of Types of  $n$ -dimensional semisimple and cosemisimple Hopf algebras is finite, *J. Algebra* **193**(1997), 571-580.
- [30] K. Yamazaki, On projective representations and ring extensions of finite groups, *J. Fac. Science Univ. Tokyo, Sect. I* **10**(1964), 147-195.
- [31] Y. Zhu, Hopf algebras of prime dimension, *Intenat. Math. Res. Notices* **1**(1994), 53-59.

DEPAUL UNIVERSITY, CHICAGO, IL 60614

*E-mail address:* lkrop@depaul.edu